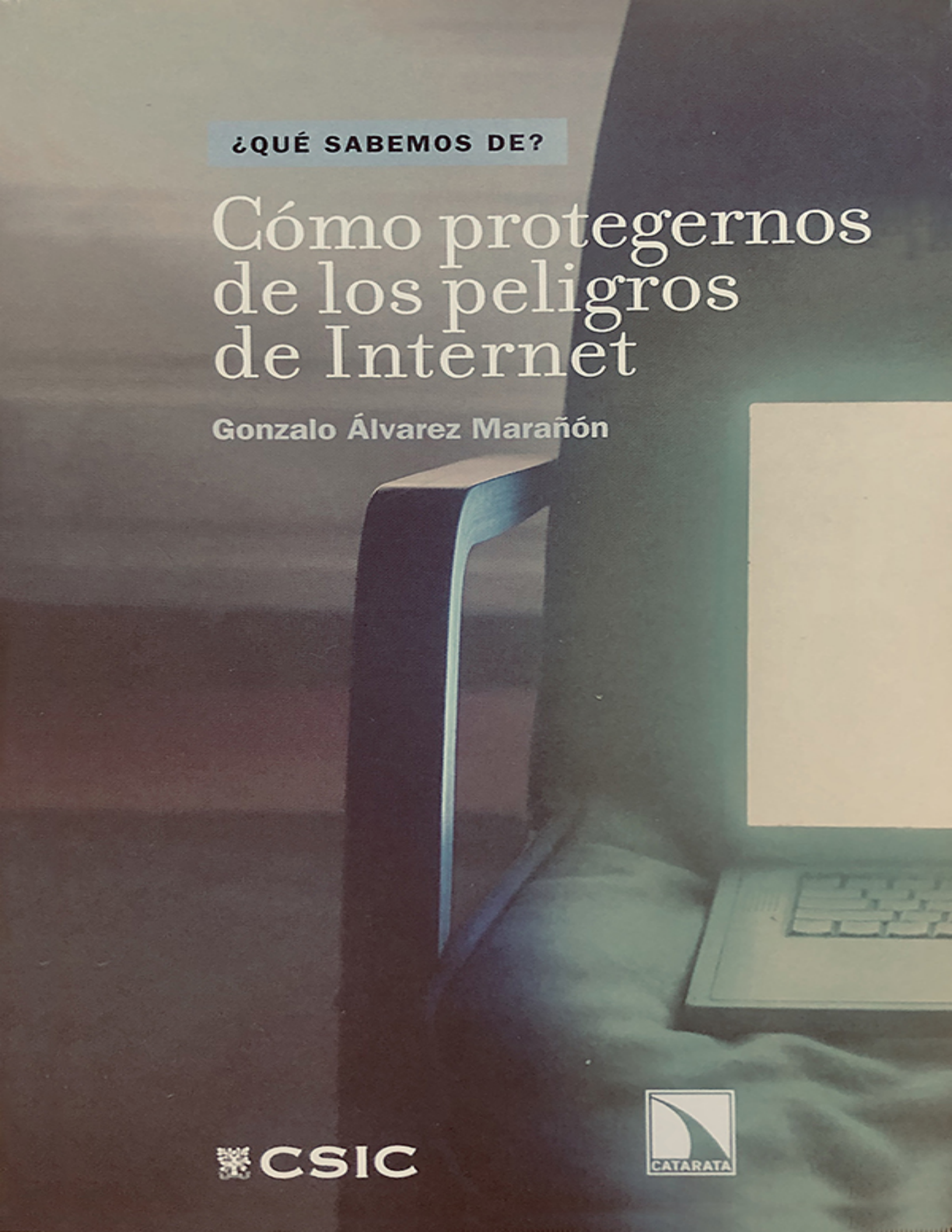
¿QUÉ SABEMOS DE?

Cómo protegernos de los peligros de Internet

Gonzalo Álvarez Marañón



CSIC

CATARATA

Cómo protegernos de los peligros de Internet

Gonzalo Álvarez Marañón

Consejo Superior de Investigaciones Científicas

Los Libros de la Catarata

Colección ¿Qué sabemos de?

COMITÉ EDITORIAL

Pilar Tigeras Sánchez, Directora
Pía Paraja García, Secretaria
Carlos Duarte Quesada
Beatriz Hernández Arcediano
Rafael Martínez Cáceres
Alfonso Navas Sánchez
José Manuel Prieto Bernabé
Miguel Ángel Puig-Samper Mulero
Javier Senén García

CONSEJO ASESOR

Matilde Barón Ayala
José Borrell Andrés
Elena Castro Martínez
Miguel Delibes de Castro
José Elguero Bertolini
Bernardo Herradón García
Pilar Herrero Fernández
Manuel de León Rodríguez
Eulalia Pérez Sedeño
Amparo Querol Simón

Catálogo general de publicaciones oficiales

http://www.060.es

Diseño gráfico de cubierta: Carlos Del Giudice

© Gonzalo Álvarez Marañón, 2009

© CSIC, 2009

© Los Libros de la Catarata, 2009

Fuencarral, 70

28004 Madrid

Tel. 91 532 20 77

www.catarata.org

ISBN (CSIC): 978-84-00-08877-4

ISBN (CATARATA): 978-84-8319-449-2

E-ISBN: 978-84-9097-878-8

NIPO: 472-09-145-4

DEPÓSITO LEGAL: M-38.532-2009

ESTE LIBRO HA SIDO EDITADO PARA SER DISTRIBUIDO. LA INTENCIÓN DE LOS EDITORES ES QUE SEA UTILIZADO LO MÁS AMPLIAMENTE POSIBLE, QUE SEAN ADQUIRIDOS ORIGINALES PARA PERMITIR LA EDICIÓN DE OTROS NUEVOS Y QUE, DE REPRODUCIR PARTES, SE HAGA CONSTAR EL TÍTULO Y LA AUTORÍA.

Glosario

Adware: todo *software* que se financia a través de publicidad más o menos visible o intrusiva. Al aceptar su licencia puede estar autorizándose al *software* a recabar información personal.

Anonimizador: *software* utilizado para navegar anónimamente por Internet sin dejar rastro.

AP *(Access Point):* véase Punto de acceso.

Banners: mensajes publicitarios en forma de carteles de tamaño variable presentes en la mayoría de páginas web y programas *adware.*

Blog: también conocido como bitácora, es un sitio web periódicamente actualizado que recopila cronológicamente textos o artículos de uno o varios autores, apareciendo primero el más reciente, donde el autor conserva siempre la libertad de dejar publicado lo que crea pertinente. Los lectores pueden dejar sus comentarios.

Botnet: red o grupo de ordenadores previamente comprometidos, denominados *bots* o *zombies,* controlados por el propietario de la misma. El propietario envía instrucciones a los *zombies* típicamente a través de IRC. Estas órdenes pueden incluir la propia actualización del *bot* o el lanzamiento de ataques contra blancos previamente seleccionados por el propietario de la *botnet.* Suelen alquilarse para cometer fechorías.

Certificado digital: documento digital mediante el cual una tercera parte de confianza, denominada autoridad de certificación, garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

Estos certificados permiten verificar la identidad de sus titulares en transacciones realizadas a través de Internet y también la verificación de firmas electrónicas.

Chat: conversación o charla entre dos o más usuarios a través de medios telemáticos utilizando el navegador web o programas específicos. Los más sofisticados incluyen la posibilidad de utilizar vídeo y voz.

Ciberacoso: acoso a través de medios telemáticos de un adulto a un menor, generalmente con fines sexuales.

Ciberatacantes: personas que utilizan Internet para realizar ataques contra sistemas de información.

Ciberbullying: acoso entre iguales en Internet, incluyendo actuaciones de chantaje, vejaciones e insultos de unos niños a otros niños.

Ciberdelincuentes: delincuentes que utilizan Internet para cometer sus crímenes.

Control parental: software para controlar lo que hacen otros usuarios, normalmente menores, cuando utilizan el ordenador sin supervisión paterna.

Correo basura: correo electrónico no solicitado, normalmente con contenido publicitario a menudo rozando el fraude, que se envía de forma masiva. Como mínimo provocan pérdidas de tiempo y recursos. En el caso peor, son ve-hículo de malware y fraudes como el phishing.

Cortafuegos: sistema de protección para filtrar según un conjunto de reglas el tráfico que entra o sale de un ordenador o una red informática.

Cracker: posee los conocimientos de los hackers, pero los utiliza para atacar sistemas informáticos, robar información y causar daños. Responsable de la mala imagen de los hackers en la mayoría de entornos sociales.

Cracking: acción y efecto de utilizar técnicas de hacking para causar daños

y robar información.

Firewall: véase Cortafuegos.

FNMT (Fábrica Nacional de Moneda y Timbre): a través de su departamento CERES (Certificación Española), la FNMT se erige como Autoridad de Certificación para autentificar y garantizar la confidencialidad de las comunicaciones.

FTP *(File Transfer Protocol):* el Protocolo de Transferencia de Archivos sirve para conectarse a un servidor y descargar archivos desde él o enviarle archivos. Existen programas específicos para transferir archivos mediante FTP, aunque los navegadores también lo soportan para descarga.

Grooming: conjunto de estrategias que una persona adulta desarrolla para ganarse la confianza del menor a través de Internet con el fin último de obtener concesiones de índole sexual.

Gusano: programa que explota vulnerabilidades en servidores de Internet para propagarse automáticamente.

Hacker: experto en informática, con conocimientos tan elevados que podría penetrar en sistemas de información ajenos y causar grandes daños. Sin embargo, los verdaderos hackers no explotan su conocimiento para cometer fechorías, actividades delictivas más propias de los crackers.

Hacking: acción y efecto de penetrar en sistemas informáticos explotando vulnerabilidades técnicas.

Ingeniería social: utilización de la picaresca para engañar a los usuarios, haciéndoles revelar datos sensibles o realizar acciones que ponen en peligro la seguridad de su información.

INTECO (Instituto Nacional de Tecnologías de la Comunicación): plataforma para el desarrollo de la sociedad del conocimiento a través de proyectos del ámbito de la innovación y la tecnología.

IP, dirección: conjunto de cuatro números que identifican a un equipo

conectado a Internet. Funciona de manera análoga a los números de teléfono. Todo equipo conectado a Internet cuenta con una dirección IP para poder enviar y recibir información.

IRC *(Internet Relay Chat):* protocolo de comunicaciones para charlas entre dos personas o en grupo.

Key logger: literalmente, registrador de teclas. Su misión consiste en registrar todas las pulsaciones de teclado de un usuario, principalmente con el fin de obtener contraseñas y datos confidenciales. Pueden estar fabricados como software o hardware, siendo los primeros utilizados por el spyware y otros troyanos y programas espía.

LOPD (Ley Orgánica de Protección de Datos): tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar.

MAC *(Media Access Control):* dirección de control de acceso al medio, compuesta por un número de 48 bits, único para cada dispositivo que se conecte a una red.

Malware: software malicioso que afecta negativamente a la seguridad de la información. Incluye a los virus, gusanos y troyanos.

Microblog: se trata de un blog con anotaciones muy breves que permiten informar en pocas palabras sobre lo que estás haciendo. Se han popularizado con Twitter. Se encuentran a medio camino entre el blogging y la mensajería instantánea.

NAT *(Network Address Translation):* la Traducción de Dirección de Red es un mecanismo utilizado por routers para intercambiar paquetes entre dos redes. Todos los equipos detrás del router poseen unas direcciones IP válidas en la red interna y gracias a NAT se traducen estas direcciones a otras válidas en Internet.

Nick: apodo o pseudónimo. Es muy frecuente utilizarlos en las redes

sociales para ocultar la identidad real.

P2P *(Peer To Peer):* las redes P2P permiten compartir archivos entre distintos equipos, de manera que unos usuarios pueden descargar los archivos del tipo que sea compartidos por otros usuarios de la red. BitTorrent y eMule son los programas más populares para P2P.

Phisher: programa o persona que perpetra ataques de phishing.

Phishing: moderna forma de fraude en el que se intenta robar la identidad de un usuario. Por medio de correos electrónicos u otro canal, se le incita a visitar una página web donde se le solicitan sus credenciales de acceso a algún servicio, normalmente financiero. Posteriormente, el phisher accederá a dicho servicio suplantando al usuario, obteniendo el máximo beneficio económico.

PIN *(Personal Identification Number):* contraseña numérica secreta que permite a un usuario autenticarse ante un sistema.

Popups: ventanas publicitarias creadas por los navegadores y otros programas, que pueden llegar a resultar verdaderamente molestas cuando su número crece descontroladamente.

Programa espía: software instalado en nuestro equipo sin nuestro conocimiento ni consentimiento, cuya misión consiste en robar y transmitir información personal, como hábitos de navegación y uso del ordenador, páginas visitadas, gustos, contraseñas, información financiera, etc. Suele considerarse una forma de troyano.

Protocolo: conjunto ordenado de pasos que hay que seguir para lograr una comunicación. Los numerosos protocolos de Internet permiten que puedan prestarse servicios tan variados como navegación, envío y recepción de correo electrónico, descarga de archivos, chat, mensajería instantánea, telefonía, etc.

Punto de acceso (AP): dispositivo hardware que interconecta dispositivos inalámbricos para formar una red inalámbrica. Normalmente un AP

también puede conectarse a una red cableada y puede transmitir datos entre los dispositivos conectados a la red de cable y los dispositivos inalámbricos.

Red social: sitio web que permite conocer gente y estar en contacto con tus amigos a través de Internet. Se han convertido en un fenómeno de masas, con un éxito sin precedentes. Muchos internautas han incorporado las redes sociales como un elemento fundamental de sus vidas.

Router: dispositivo hardware que administra el tráfico entre dos redes, en el caso doméstico, entre la red local del hogar e Internet.

Scam: timo enviado a través del correo electrónico.

Script kiddies: la forma más baja de cracker, ya que sin apenas conocimientos informáticos se dedican a causar daños utilizando ciegamente herramientas de hacking creadas por otros con verdaderos conocimientos.

Spam: véase Correo basura.

Spammer: programa o persona que envía spam.

Spyware: véase Programa espía.

SSL *(Secure Sockets Layer):* protocolo de transmisión de datos utilizado para proteger las comunicaciones a través de Internet entre dos equipos. Ofrece los servicios de confidencialidad de los datos, integridad de los datos y autenticación del servidor web y, opcionalmente, del cliente, mediante el uso de certificados digitales.

Troyano: programa malicioso que se instala en el ordenador de la víctima aparentando ser un programa benigno. Una vez instalado permite a un atacante el control remoto del equipo de la víctima.

URL *(Uniform Resource Locator):* secuencia de caracteres, de acuerdo a un formato estándar, usado para nombrar los recursos localizados en un servidor web, como documentos e imágenes en Internet. Por ejemplo,

http://www.servidor.com/directorio/documento.pdf.

Virus: código malicioso capaz de replicarse a sí mismo co-piándose en otros programas. Realiza acciones dañi-nas, desde la mera molestia a la destrucción masiva de datos.

WEP *(Wired Equivalent Privacy):* sistema de cifrado para redes inalámbricas Wi-Fi. Posee numerosas debilidades que permiten romperlo en minutos, por lo que se desaconseja su uso para proteger redes Wi-Fi.

WPA *(Wi-Fi Protected Access):* sistema de cifrado para redes inalámbricas Wi-Fi, creado para corregir las deficiencias del sistema previo WEP. WPA se puede considerar una migración mientras se creaba el sistema más sofisticado y seguro WPA2.

WPA2: sistema de cifrado para redes inalámbricas Wi-Fi, que mejora la seguridad de su predecesor WPA. Se trata de la opción más segura si está soportada por todas las estaciones de la red Wi-Fi.

Zombie: ordenador comprometido por un ciberatacante e integrado dentro de una botnet.

Introducción

Internet sí, pero con seguridad

Internet está transformando nuestra concepción del mundo y revolucionando nuestras vidas. Gracias a Internet podemos relacionarnos de formas innovadoras con personas en el otro extremo del planeta, compartir fotos y vídeos instantáneamente con familiares y amigos, obtener información sobre cualquier tema imaginable en la más fantástica *multiteca* nunca soñada, expresar nuestros talentos artísticos a la vista de millones, comprar en el bazar más gigantesco jamás creado por el hombre las mercancías más inimaginables a cualquier hora del día o de la noche. La lista es, como Internet, infinita.

Por desgracia, Internet presenta también su reverso tenebroso: intrusos, virus, timos, pederastia, mafias, piratería, espionaje… Estos males vienen a empañar la visión idílica de una red de redes donde todos colaboran y comparten información y conocimientos en paz y armonía. No podemos vivir sin Internet, pero tampoco podemos confiar ciegamente en sus bondades ni sumergirnos alocadamente en sus profundidades. Internet alberga innumerables peligros para los que afortunadamente existe protección. El miedo jamás debería hacernos renunciar a Internet.

Este libro será tu fiel compañero de viaje que te guiará para disfrutar de todas las ventajas y servicios de Internet de forma segura y sin sorpresas. En sus páginas aprenderás a identificar los riesgos más frecuentes para los usuarios domésticos y a escoger las medidas de protección más adecuadas

para cada caso. En un lenguaje sencillo y con ejemplos prácticos que a todos sirvan, se desgranarán los secretos más importantes de la seguridad en Internet.

Un libro para el usuario doméstico

La seguridad de la información reposa sobre tres patas: la tecnología, los procesos y las personas. A menudo tendemos a concentrarnos exclusivamente en la primera, olvidando las otras dos. La mejor inversión a largo plazo que puede hacerse en seguridad es concienciar, educar y formar a las personas en esta materia. Sólo así las soluciones tecnológicas como antivirus, cortafuegos, cifrado de archivos, etc., serán plenamente eficaces. Este libro busca satisfacer esa necesidad de concienciación. Está dirigido por tanto a todos aquellos usuarios domésticos o de pequeñas oficinas con escasos conocimientos de informática y con deseos de disfrutar con seguridad de las ventajas de Internet.

La práctica totalidad de usuarios domésticos, el 97% según un reciente estudio de INTECO, utiliza alguna de las numerosas variantes de Windows XP, Windows Vista o Windows 7. Otros sistemas operativos como Mac (1%) o alguno de los variados sabores de Linux (1%) registran todavía una penetración marginal en el entorno doméstico. La información proporcionada en el libro busca presentar los conceptos universales de seguridad de la información, que pueden aplicarse por igual para la protección de cualquier sistema. Se ha evitado deliberadamente hacer referencias a sistemas operativos y programas concretos: por un lado, éstos cambian con vertiginosa rapidez, lo que vuelve estas referencias obsoletas el mismo día de su publicación; por otro, a menudo el usuario se enfrasca en el uso de la herramienta concreta, perdiendo de vista los conceptos básicos detrás de su uso.

Se ofrecerán por tanto pautas y consejos para implantar las medidas de

seguridad más adecuadas, pero sin listar instrucciones para programas concretos.

Un viaje a la seguridad de la información

En el primer capítulo, se introducen mediante ejemplos sencillos una serie de conceptos tomados de la disciplina de gestión del riesgo que ayudarán al lector a comprender mejor qué medidas de seguridad deben implantarse en cada situación para satisfacer unos objetivos concretos.

En el segundo capítulo se describen cuáles son las amenazas más importantes a las que está expuesta la información de los usuarios domésticos.

En el tercer capítulo se explica en qué consisten, cómo funcionan y cómo deben implantarse las medidas de seguridad imprescindibles, sin las cuales resulta imposible garantizar la seguridad de la información.

El cuarto capítulo presta atención a otras amenazas menos graves y a las medidas de seguridad necesarias para contrarrestarlas.

El quinto capítulo presenta los problemas de las redes inalámbricas Wi-Fi, de gran penetración en los hogares, y las mejores medidas de seguridad para contrarrestarlos.

Por último, en el capítulo sexto se ofrecen una serie de consejos para utilizar con seguridad algunas de las aplicaciones más populares de Internet, como el navegador, el correo electrónico, el *chat,* las redes de descarga de archivos, etc.

Recursos sobre seguridad en Internet

A lo largo del libro se mencionan numerosos sitios web a los que acudir en busca de información o para descargar *software* y herramientas. Las direcciones web no aparecen en el texto, sino que se han agrupado en un apéndice al final para facilitar su consulta en cualquier momento. De esta

forma, podrás localizar con rapidez por ejemplo antivirus gratuitos o programas de control parental simplemente acudiendo al apéndice, en lugar de bucear en las páginas del libro.

¿Se te escapa algún concepto? Acude al glosario

En el texto aparecen muchas palabras, siglas y conceptos que pueden resultar nuevos a más de un lector. Para ayudar a una mejor comprensión, se ha añadido un glosario con las palabras más técnicas relacionadas con Internet y con la seguridad de la información. Si durante la lectura del libro no te suena alguno de los conceptos manejados, acude al glosario, seguro que lo encontrarás definido ahí.

Agradecimientos

Ningún autor escribe un libro en completa soledad. Un sinfín de personas colabora en mayor o menor medida. Quiero expresar mi agradecimiento a todos mis amigos, quienes con sus consejos, comentarios o palabras de apoyo han ayudado a que esta pequeña obra vea la luz. En particular, mil gracias a Igor Campillo Santos y a Luis Miguel Rocha Costa; a Jaime Pérez del Val, Agustín Martín Muñoz y Amalia Orúe López, del CSIC; a Vicente Aceituno Canal, de SIA; a Bernardo Quintero Ramírez, de Hispasec; al Teniente Coronel Roberto Plà, del Escuadrón de Vigilancia Aérea (EVA) número 4; a Chema Alonso Cebrián, de Informática64; a David Carrasco López, héroe certificado; a Pía Paraja y a todo el equipo de Los Libros de la Catarata; y muy especialmente a María.

CAPÍTULO 1

Qué es la seguridad de la información

¿Será seguro pagar esta compra por Internet con mi tarjeta de crédito? ¿Estaré introduciendo un virus en mi ordenador si me descargo este programa desde esta página web? ¿Están mis datos personales a salvo de intrusos? Todos los usuarios de las tecnologías de la información se formulan en uno u otro momento preguntas similares. En definitiva, ¿qué es la seguridad de la información? ¿Qué queremos decir cuando afirmamos que algo es seguro o que no lo es?

Por desgracia, existe mucha confusión: a menudo se tergiversa la seguridad con las medidas de seguridad o con un producto determinado. Son frecuentes creencias como las siguientes: "Estoy seguro porque tengo un cortafuegos" o "Si tengo un antivirus, estoy seguro, ¿no?". Desafortunadamente, la seguridad no puede reducirse a un producto, es el resultado de un proceso continuo de formulación de objetivos, implantación de medidas y revisión del cumplimiento de los mismos.

Para explicar la seguridad de la información de forma clara y sencilla en este primer capítulo se introducirán los conceptos de gestión del riesgo, contexto y expectativas de seguridad. En los apartados siguientes se analizarán con ejemplos cotidianos cada uno de ellos para comprender su importancia. Al final del capítulo, el lector estará preparado para aplicar con mayor provecho las medidas de seguridad explicadas en el resto del libro.

La vida es riesgo

En la vida cotidiana nos enfrentamos continuamente a situaciones de peligro:

- Practicamos voluntariamente deportes de riesgo, en los que puede peligrar nuestra vida o nuestra integridad personal.
- En las carreteras, ponemos nuestra vida en juego cada vez que montamos en un vehículo, siendo a veces los causantes de los accidentes y otras siendo las víctimas de los errores de otros conductores.
- Incluso en el trabajo, dependiendo de la profesión desempeñada, es posible poner en riesgo la vida cada vez que se inicia la jornada.

¿Cómo es posible afrontar este riesgo continuo en nuestras vidas? Gestionándolo.

La *gestión del riesgo* es la disciplina que nos ayuda a sobrevivir. Aunque sea de manera inconsciente, en cada situación que pueda representar un riesgo potencial evaluamos cuál es el contexto, cuáles son nuestras expectativas y qué medidas de seguridad podemos aplicar. En función de la frecuencia con que se cumplen esas expectativas en ese contexto, se considera que las medidas de seguridad son adecuadas y que el riesgo está bajo control.

A menudo estas evaluaciones se ven deformadas por ideas irracionales: por ejemplo, nos da más miedo viajar en avión que en coche, cuando estadísticamente está demostrado que el avión es más seguro. El problema radica en que cuando se produce un accidente aéreo mueren cientos de personas a la vez, aparece en titulares de prensa y televisión, causándonos un desasosiego mayor que las docenas de muertos en carreteras en un solo fin de semana. En nuestra mente está más disponible lo infrecuente, pero aparatoso, que lo cotidiano, pero anodino. Como consecuencia, nuestra

sensación de riesgo no suele coincidir con la realidad, lo que nos conduce a tomar decisiones equivocadas. Por eso resulta tan difícil gestionar el riesgo adecuadamente en nuestras vidas.

Veámoslo con otro ejemplo. No nos preocupa beber del grifo de nuestras casas, pero no beberíamos del grifo en un país con aguas de dudosa potabilidad. Cuando bebemos, nuestra expectativa es saciar la sed con un agua pura. Esta expectativa se cumple en el contexto del hogar, pero para que se cumpla en el contexto de un país con alto nivel de exposición a contaminantes y bacterias, se adoptan medidas de seguridad como hervir el agua, utilizar filtros o pastillas potabilizadoras. Sin embargo, habrá personas que por no gastar en agua embotellada se arriesgarán a contraer una enfermedad que a la larga les costará infinitamente más, incluso la vida.

En definitiva, nos consideramos seguros cuando esperamos que nuestras expectativas se cumplan en una situación determinada. El cumplimiento repetido de nuestras expectativas refuerza nuestra sensación de seguridad.

Expectativas

Nuestra actividad diaria con los sistemas informáticos está plagada de expectativas:

- Cuando encendemos el ordenador, esperamos que éste funcione, que el disco duro no se haya estropeado ni se hayan perdido los datos, y que toda la información con la que estuvimos trabajando el día anterior permanezca aún en su sitio.
- Si se tienen menores bajo nuestra tutela, esperamos que no visiten sitios en la Red de contenidos inadecuados.
- En el uso cotidiano de los distintos servicios de Internet, como el correo electrónico, el *chat* o la navegación, esperamos una cierta garantía de nuestra privacidad, de manera que nadie sepa por

dónde navegamos, con quién “chateamos” o qué correos hemos recibido.

Ahora bien, por lo general, estas expectativas no tienen por qué cumplirse: el disco duro puede estropearse y perderse toda su información o un virus podría borrar su contenido; a nuestras espaldas, y sin nuestro conocimiento, los usuarios podrían estar navegando por sitios desaconsejables; todos nuestros mensajes de correo podrían ser interceptados y leídos o toda nuestra actividad de navegación espiada.

Que la mayoría de las veces estas expectativas se cumplan sin necesidad de tomar ninguna acción especial no significa que siempre deba ser así. Para garantizar su cumplimiento de manera continuada en el tiempo se vuelve imprescindible implantar una serie de controles o medidas de seguridad adecuadas al contexto de operación.

Contextos

La seguridad depende fuertemente del contexto. Por ejemplo, no nos asusta pasear de día por un parque repleto de turistas, pero posiblemente no nos atreveríamos a transitarlo de noche y sin un alma. Se trata del mismo parque, sí, pero la hora del día y el volumen de visitantes, es decir, el contexto, afectan al tipo y número de amenazas presentes que podrían evitar que se cumpliera nuestra expectativa de pasear plácidamente. Esta sensación subjetiva de riesgo puede verse afectada irracionalmente si tenemos noticia de un asesinato cometido en el parque.

En cuanto a la seguridad de la información, queda claro que no son iguales las amenazas, vulnerabilidades y riesgos existentes en un hogar, en una empresa o en un banco. Las medidas de seguridad que pueden resultar útiles en un contexto, por ejemplo en una empresa, serán excesivas para un hogar e insuficientes para un banco. A pesar de que se trata de las mismas

medidas, en función del contexto donde se apliquen varía su eficacia.

A menudo se observan sistemas informáticos en los que se han implantado medidas de seguridad sin ton ni son, simplemente porque son muy buenas o porque otros las tienen. Sin embargo, previamente a la instalación de una medida de seguridad, debe evaluarse si será capaz de cumplir las expectativas la mayor parte del tiempo en el contexto en el que será utilizada. Sólo así protegerá eficazmente frente al riesgo identificado.

Contexto y expectativas en el hogar

El contexto en el hogar suele poseer las siguientes características:

- La población de usuarios es mixta: está compuesta por adultos, jóvenes y niños.
- Se poseen conocimientos limitados sobre informática y en especial sobre seguridad.
- Se dispone de conexión a Internet por ADSL, cable o módem telefónico.
- Los recursos económicos son limitados.
- La finalidad principal de los ordenadores suele ser el ocio y el entretenimiento.

Las expectativas más frecuentes en un entorno doméstico incluyen, pero no se limitan a:

- Evitar que entren usuarios no autorizados. (La amenaza de los intrusos se analiza con detalle en el capí-tulo 2.)
- Impedir infecciones de virus informáticos. (Los virus se describen en el capítulo 2.)
- Evitar los fraudes y timos. (Éstos se tratan en el capítulo 2.)

- Mantener a raya el *spam* (correo basura o correo no deseado). (El *spam* se aborda en el capítulo 4.)
- Controlar el uso de Internet que hacen otros usuarios, especialmente los menores. (En el capítulo 4 se repasará este problema.)
- Ser capaz de recuperarse tras desastres informáticos que hacen perder datos del disco. (Los fallos de *software* y *hardware* se tratan en el capítulo 4.)
- Controlar el acceso al equipo y a sus archivos por los distintos miembros de la familia. (Este tema se explica en el capítulo 4.)
- Limitar la ejecución incontrolada de *software* en el equipo. (Se verá cómo hacerlo en el capítulo 4.)
- Proteger hasta cierto punto razonable la privacidad. (La protección de la privacidad y del anonimato constituyen el núcleo del capítulo 4.)
- Evitar que los vecinos tengan acceso a Internet utilizando mi conexión inalámbrica. (Las cuestiones de seguridad relacionadas con el uso de redes inalámbricas se consideran en el capítulo 5.)
- Navegar por Internet sin sobresaltos de seguridad. (En el capítulo 6 se ofrecen pautas para una navegación responsable.)
- Enviar y recibir correos sin que nadie los intercepte y "chatear" con los amigos sin ser molestado. (El sentido común en el uso de la mensajería se reivindica en el capítulo 6.)
- Intercambiar archivos libres de virus con otros usuarios a través de redes de intercambio, como eMule. (Estas redes se revisan en el capítulo 6.)

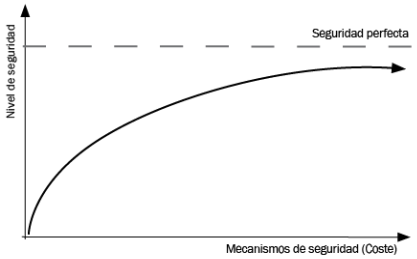
En los capítulos referidos se explicará qué tipo de amenazas pueden frustrar estas expectativas y qué medidas de seguridad pueden combatirlas.

Inversión en seguridad

Una vez analizado el contexto y comprendidas las expectativas, el siguiente paso consiste en plantearse cuáles son las medidas de seguridad que cabe implantar. Para tomar esta decisión es necesario entender previamente cuáles son las amenazas a las que se está expuesto y de qué manera explotan las vulnerabilidades de los sistemas de información.

La buena noticia para los usuarios domésticos es que con una pequeña inversión en tiempo y dinero es posible aumentar drásticamente el nivel de seguridad alcanzado. Todos los sistemas operativos incluyen de forma predeterminada numerosas herramientas de seguridad, a menudo desconocidas o poco usadas. Además, la seguridad predeterminada que el sistema operativo es capaz de proporcionar puede suplementarse con numerosas herramientas de terceros que en la mayoría de los casos pueden utilizarse gratuitamente o con un mínimo desembolso.

FIGURA 1



Aunque por mucho que se gaste nunca podrá alcanzarse la seguridad perfecta, basta un pequeño esfuerzo en la implantación de mecanismos de seguridad para lograr un nivel de seguridad más que aceptable en el entorno doméstico.

No toda la información es igualmente valiosa

Obviamente, cuando se habla de seguridad de la información, el activo que

se ha de proteger es la información. Ahora bien, no toda la información posee el mismo valor para todo el mundo. En primer lugar, es necesario determinar el valor de dicha información, tanto la que reside en nuestro sistema como aquella a la que nuestro sistema nos permite acceder:

- Existen activos sin valor para otras personas, como las fotos del bebé o esos poemas de juventud.
- Existen activos con gran valor para otras personas, como información de tarjetas de crédito o contraseñas de acceso al banco.
- Existen servicios de gran valor para el usuario, como poder acceder a páginas web o al correo electrónico.

Por tanto, para poder gestionar adecuadamente el riesgo es necesario listar cuáles son los diferentes activos de información, así como el valor estimado de cada uno, quedando claro que el valor es una magnitud totalmente subjetiva. Por supuesto, este análisis no tiene por qué ser cuantitativo, es decir, no hace falta asignar un valor monetario concreto a cada activo, lo que en muchos casos sería imposible: ¿cómo valorar esa base de datos de recetas de cocina que costó diez años compilar?

El análisis puede ser cualitativo. En este caso, se procede asignando a cada activo un valor: desde 1 para lo que tiene poco valor o es fácilmente reemplazable hasta 10 para lo que tiene un gran valor económico o sentimental o es irremplazable. Una vez compilada la lista y ordenada por el valor de cada activo, se podrá dedicar más esfuerzo a proteger aquello cuyo valor sea mayor o cuya exposición sea más evidente.

No se trata de pasar tardes enteras clasificando datos por su valor, sino de dedicar algún tiempo a reflexionar sobre qué tipo de datos guardamos en nuestro ordenador o qué tipo de servicios nos presta y cuál es su valor

subjetivo para nosotros. El objetivo de este ejercicio es tomar conciencia de qué es importante y qué no con el fin de utilizar los mecanismos adecuados para proteger lo que más nos importa. (Estos mecanismos se explicarán más adelante a lo largo del libro.) Este ejercicio nos ayuda a seleccionar los mecanismos necesarios para nuestro contexto concreto y para nuestras expectativas.

Algunos ejemplos de activos encontrados típicamente en un ordenador doméstico incluyen:

- Archivos multimedia propios: los vídeos caseros y las fotografías rápidamente llenan el disco. Normalmente sólo poseen valor para su dueño. La mayoría son irreemplazables: nunca se regresará de vacaciones a ese lugar ni se repetirá esa boda o bautizo.
- Archivos multimedia de terceros: películas, música, audiolibros, libros electrónicos, fotografías de *stock.* Pueden poseer valor para más personas que el dueño. Aunque en su mayoría son reemplazables, implicaría un coste económico.
- Archivos ofimáticos: documentos de texto, hojas electrónicas, bases de datos. No suelen poseer valor para otras personas. El dueño ha podido invertir muchas horas en su creación, por lo que a menudo son irremplazables o el coste de reemplazo sería elevadísimo.
- Información financiera: datos personales y fiscales, números de cuentas bancarias, tarjetas de crédito, declaración de la renta. La información posee gran valor para otras personas. Es muy fácilmente reemplazable.
- Contraseñas de acceso a servicios en Internet: poseen gran valor para otras personas. Son fácilmente reemplazables.
- Acceso a Internet: dependiendo del tipo de usuario, puede ser

inadmisible prescindir de la conexión durante unas horas o puede ser totalmente prescindible. El reemplazo puede ser difícil.

- Equipo informático: el valor del propio equipo informático junto con sus periféricos dependerá igualmente del tipo de uso al que esté destinado. No es lo mismo usarlo para juegos que para trabajar. El impacto de la interrupción de servicio será variable según la finalidad. Su reemplazo tiene un coste económico asociado.

Uno debe preguntarse: ¿me afectaría negativamente la pérdida de estos datos o de este servicio? En tal caso, ¿qué puedo hacer para evitar perderlos? En función del valor de esos datos o del coste de reemplazo, se deberán extremar las precauciones, implantando las medidas de seguridad que mejor contrarresten las amenazas. Estas medidas se explicarán en los siguientes capítulos.

No toda la información está expuesta a los mismos peligros

Para gestionar adecuadamente el riesgo no sólo hay que tener en cuenta el valor de los activos, sino también su exposición: si ésta es pequeña, el riesgo asociado será igualmente bajo. Si la exposición es grande, entonces el riesgo aumentará. Veámoslo con un ejemplo.

Un profesional liberal trabaja desde su casa. El ordenador y la conexión a Internet constituyen sus herramientas de trabajo. Su expectativa de seguridad principal consiste en que tanto el ordenador como la conexión a Internet funcionen ininterrumpidamente en horas de trabajo, ya que cada hora de caída del servicio está parado perdiendo dinero. Si vive en un área urbana grande con suministro eléctrico estable y servicio de Internet de alta calidad, puede confiar en que el riesgo de interrupción del servicio es bajo. Sin embargo, en un área rural, donde los apagones son frecuentes y la

conexión a Internet se presta con intermitencia, la exposición a este riesgo es muy elevada. El valor subjetivo del activo es idéntico para él tanto si vive en la ciudad como si vive en el campo; sin embargo, el grado de exposición varía de un emplazamiento a otro y, por consiguiente, el nivel de riesgo es mayor en el segundo caso.

El grado de exposición puede aumentar por muchos motivos:

- Con el número de personas que utilizan un ordenador: cuantos más usuarios, mayor número de imprudencias.
- Con el tipo de sistema operativo: admitamos que algunos sistemas operativos registran una mayor incidencia de ataques de *ciberdelincuentes* y virus. (De todo ello se hablará extensamente en el próximo capítulo.)
- Con el desconocimiento: dicen que la ignorancia es atrevida. Algunos usuarios no comprenden el verdadero peligro de Internet. "El que no sabe es como el que no ve." Muchas imprudencias se cometen por puro desconocimiento.

Por lo tanto, a la hora de valorar los riesgos debe intentar introducirse en la ecuación a la exposición: cuanto mayor sea el grado de exposición, mayor será el riesgo.

Ni que decir tiene que el grado de exposición depende fuertemente del contexto. Cuando yo era niño y visitaba en verano el pueblo de mi madre, dejaba por la noche los juguetes y la bicicleta tirados en la calle y todo seguía allí al día siguiente. Prueba a dejar la bicicleta en una plaza de una gran capital y vuelve al día siguiente a ver si está.

Resumen

Para sobrevivir en este mundo nos valemos diariamente de la gestión del

riesgo: desde pasear por el parque hasta beber agua del grifo, continuamente nos vemos obligados a evaluar posibles peligros y a tomar decisiones sobre cómo actuar, a menudo de forma irracional. La gestión del riesgo implica la creación de unas expectativas u objetivos de seguridad, adecuados a un contexto determinado, para cuyo cumplimiento necesitaremos frecuentemente el uso de medidas protectoras. Para saber cuándo aplicar estas medidas es necesario analizar el valor de la información y de los servicios que deseamos proteger, así como su nivel de exposición. De esta manera, dedicaremos más recursos a proteger lo que tiene más valor para nosotros o lo que está más expuesto.

En el capítulo 2 se explicará frente a quién debemos proteger esos activos y, en los siguientes, las medidas de protección más adecuadas.

CAPÍTULO 2

Amenazas a la información

Cuando uno practica deportes de riesgo o conduce el coche, parece evidente dónde está el peligro. Uno ve de dónde proviene la amenaza y es consciente de su propia vulnerabilidad. De ahí que resulte relativamente sencillo tomar precauciones.

Sin embargo, cuando conectamos el ordenador a Internet no está tan claro de dónde viene el peligro.

Se han oído tantas noticias y leyendas urbanas sobre virus y *hackers* que todo aparece confuso. ¿Cuáles son las amenazas? ¿Qué puede pasarnos? ¿Contra quién o qué debemos protegernos?

En este capítulo se repasarán las amenazas más importantes que hoy se afrontan en entornos domésticos:

- Los *ciberatacantes*.
- El *software* malicioso o *malware*.
- Los fraudes y timos.
- Otras amenazas, tal vez menos llamativas, pero no por ello menos temibles, como los cortes de luz o las averías del *hardware.*

‘Ciberatacantes’

Muchos usuarios particulares consideran que se encuentran a salvo de los *ciberatacantes* porque no poseen ningún secreto comercial ni político, ni sus archivos interesan a nadie. “No hay nada de valor en mi ordenador”,

alegan, “¿por qué alguien iba a querer entrar en él? Y, además, ¿cómo iban a encontrarme?”. Estos argumentos resultan completamente falaces, como se demostrará a continuación.

Qué tengo de valor para un ‘ciberatacante’

Todo usuario conectado a Internet, por modestos que sean sus recursos, posee cuatro importantes activos para el *cibera-tacante:*

1. Espacio de disco: quien más quien menos, todo usuario cuenta ya con 500 GB de disco o más.
2. Potencia de cálculo (CPU): los últimos equipos vienen ya dotados de potentes procesadores de doble y hasta cuádruple núcleo y velocidades mínimas de 2 GHz.
3. Ancho de banda: la conexión ha ido mejorando paulatinamente y los hogares españoles hoy se conectan en su mayoría a través de ADSL o cable, con velocidades mínimas de descarga de 2 Mbps.
4. Cuenta bancaria e información financiera y fiscal: si alguien tiene ordenador y banda ancha contratada, entonces también tiene una cuenta bancaria y datos personales como nombre, apellidos, DNI, contraseñas, tarjetas de crédito, incluso un certificado digital de la Fábrica Nacional de Moneda y Timbre (FNMT), usado para autenticarse ante la Administración. Además, seguro que hace la declaración de la renta.

Típicamente, los usuarios domésticos no son el blanco deliberado de un atacante que vuelca en su realización todos sus recursos, sino que sucumben víctimas de ataques indiscriminados en busca de recursos informáticos e información personal.

Quiénes son los ‘ciberatacantes’

Durante los años setenta y ochenta, los *hackers* eran, fundamentalmente, gente con profundos conocimientos de informática. Dado que, como dice el adagio, "la información es poder", con el tiempo fueron estos expertos los capacitados para colarse en sistemas informáticos, ya que sabían todo lo que podía saberse sobre ordenadores y protocolos de comunicación, y conocían sus debilidades y cómo explotarlas. También resultó muy extendido en esta época el fraude telefónico *(phreaking)*. El *hacking* alcanzó cotas de popularidad inusitadas gracias a una película de culto: *Juegos de guerra,* de John Badham, la cual impulsó la creación de la subcultura *hacker*.

Durante la década de los noventa, los *hackers* y creadores de virus se integraban en comunidades *underground* de jóvenes rebeldes y a menudo inadaptados. Atacaban sistemas informáticos con el objetivo de obtener mayor conocimiento sobre su funcionamiento, ganar notoriedad, concienciar a la sociedad de las vulnerabilidades de las redes, divertirse… La creación del *malware* o el acto de *hackear* en sí mismos constituían el delito. Es entonces cuando se comienza a asociar el *hacking* con la delincuencia. Se crea la división entre el *cracker* y el *hacker:* el primero sería el "*hacker* malo*"*, que busca causar daños deliberados o lucrarse gracias al *hacking,* mientras que el *hacker* a secas seguiría siendo el "*hacker* bueno*"* o "*hacker* ético*"*, quien pone sus conocimientos al servicio de la sociedad. A los *hackers* malos también se les suele denominar "sombreros negros" *(black hats)*, en alusión al color del sombrero del malo en las viejas películas del oeste. En esta época aparecen también los *script kiddies,* la forma más baja de *cracker,* niñatos que crean daños y atacan redes con programas *(scripts)* escritos por otros y cuyo funcionamiento a menudo ni siquiera comprenden.

A partir del año 2004 culmina la época romántica de los *hackers.* Hoy

han conquistado el término meros *ciberdelincuentes,* quienes han edificado una verdadera industria con niveles muy altos de profesionalidad y conocimientos, muy bien organizados y con el afán de lucro como motivación detrás de sus crímenes. Se han especializado extraordinariamente, forjándose alianzas estratégicas entre *spammers, phishers, crackers* y creadores de virus. Es el nuevo crimen organizado. Existe un floreciente supermercado *undernet* que mueve miles de millones de dólares al año y donde todo está en venta: vulnerabilidades sin publicar, números de tarjeta de crédito robados, cuentas bancarias con claves de acceso, certificados de la FNMT con su PIN, alquiler de *botnets,* etc. Esta creciente profesionalización del delito informático constituye una de las mayores preocupaciones de los expertos en seguridad de la información y de los cuerpos de seguridad de los Estados.

Para qué me quieren los 'ciberatacantes'

Existen infinitas razones por las que un *ciberatacante* puede desear atacar a desprevenidos y suculentos usuarios domésticos:

- Lucro. Credenciales de acceso a aplicaciones bancarias, números de tarjeta de crédito, certificados de la FNMT, todos esos datos se pueden vender para lucrarse a partir de ellos.
- Utilizar miles de pequeños ordenadores como el de la víctima para atacar coordinadamente a grandes servidores, con el fin de socavar la disponibilidad del blanco atacado, de manera que deje de funcionar. Yahoo!, Amazon o eBay han sido en el pasado objeto de este tipo de ataques. Piénsese en el impacto de interrumpir el servicio de Gmail durante unas horas.
- Atacar otros ordenadores desde el de la víctima, que es utilizado como puente de ataque. De esta manera, todos los rastros de

auditoría en el servidor final atacado señalarán a ese ordenador y no al del atacante. Hasta cierto punto, somos responsables de mantener nuestro ordenador seguro para evitar que otros usuarios sean atacados desde nuestro equipo.

- Realizar ataques de robo de identidad *(phishing)* contra otros usuarios.
- Enviar correo basura *(spam)*. Por modesto que sea nuestro ancho de banda, se pueden enviar desde equipos domésticos millones de correos basura.
- Instalar servidores de *software* pirata o de películas o de música. En muchas empresas y hogares, el ancho de banda parece decaer rápidamente y un buen día se encuentran con que no queda espacio libre en disco. Buscando, buscando, ¿qué se descubre? Que en un directorio perdido existe toda una colección de *software* pirata, a la que se accedía mediante un servidor de FTP que la víctima nunca instaló.
- Iniciación. Muchos *ciberatacantes* inician su aprendizaje con blancos fáciles, como ordenadores domésticos totalmente desprotegidos. Después dan el salto a pequeñas empresas, también mal protegidas. Y de ahí van escalando lentamente a medida que maduran sus habilidades.

Cómo pueden encontrarme

Otro error común consiste en pensar que nadie nos conoce, que por no tener página *web* ni *blog* ni nada similar, ningún *ci- beratacante* puede llegar a descubrirnos. Y así es. Ningún *ciberatacante* nos conoce individualmente, ni falta que le hace. Lo que conocen es nuestra dirección IP. Para el *ciberatacante,* la nuestra es una dirección IP más, dentro de un rango

aleatorio que está escaneando con alguna herramienta automatizada. El tiempo medio que transcurre desde que un ordenador se enciende y se conecta a Internet hasta que comienza a ser atacado es de unos pocos segundos. En otras palabras, sea cual sea nuestra dirección IP, sin importar si es dinámica (una IP diferente cada vez que nos conectamos) o estática, en un par de segundos ya estaremos siendo atacados.

DIRECCIONES IP

Del mismo modo que todo teléfono debe poseer un número para poder llamar y ser llamado, toda máquina presente en Internet debe tener asignada una dirección IP que la identifique de manera unívoca entre todos los millones de máquinas en la Red. Esta dirección es un prerrequisito insoslayable para poder acceder a los servicios de Internet.

Cada vez que te conectas a Internet a través de un acceso telefónico, tu proveedor de servicio te proporciona una dirección IP distinta, por lo que se le suele llamar IP flotante o dinámica. Por el contrario, si utilizas una conexión por ADSL o cable, normalmente siempre tendrá asignada la misma dirección IP, aunque en los últimos años se tiende a asignarle igualmente una IP dinámica cada vez que establece la conexión.

La forma estándar de expresar las direcciones IP consiste en utilizar cuatro grupos de números separados por puntos. Cada grupo de números toma un valor entre 0 y 255, como por ejemplo 80.24.172.100.

Los *ciberatacantes,* especialmente los aficionados *(script kiddies)*, no suelen atacar blancos concretos, sino blancos aleatorios comprendidos dentro de un rango de direcciones IP. Por eso seremos atacados inexorablemente: por poseer una dirección IP, no por ser quienes somos.

Cómo atacan los 'ciberdelincuentes'

Un sistema informático está compuesto de *software* (sistema operativo, aplicaciones de escritorio, programas variados, etc.), de *hardware* (PC, monitor, impresora, escáner, discos externos, etc.) y de personas que los manejan. No hay magia en cómo los *ciberatacantes* penetran en los sistemas informáticos; el secreto reside en explotar sus vulnerabilidades. Una vulnerabilidad no es más que una debilidad presente en un sistema.

Ahora bien, que exista una vulnerabilidad no es sinónimo de que vaya a materializarse un ataque, todo dependerá de la dificultad de explotarla. Por ejemplo, una ventana abierta en una casa es una vulnerabilidad. Pero no es lo mismo que esté abierta la ventana de una planta baja que la de un sexto piso. La dificultad de explotación varía drásticamente.

¿De dónde proceden las vulnerabilidades de los sistemas informáticos? Sobre todo de dos fuentes:

- Fallos de programación: todos los sistemas operativos y todo el *software* en general presentan errores de programación. Algunos de ellos poseen un impacto negativo para la seguridad, ya que permiten a un atacante ejecutar comandos o acceder a información del sistema afectado. Estos fallos están presentes en los productos adquiridos al fabricante. Lo único que se puede hacer para protegerse frente a ellos es aplicar los parches que periódicamente publica el fabricante para corregir las vulnerabilidades detectadas. (Las actualizaciones se tratan en el siguiente capítulo.)
- Configuración deficiente: un sistema, por muy robusto que sea, puede estar mal configurado. Puedo tener una puerta blindada en mi casa pero, si dejo las llaves debajo del felpudo, no habré aumentado mucho mi seguridad. Igualmente, los sistemas informáticos pueden configurarse deficientemente: usar contraseñas débiles, garantizar excesivos privilegios a usuarios que no los necesitan, activar servicios innecesarios, etc. La mala configuración es ya responsabilidad del usuario, si bien es verdad que algunos productos vienen de fábrica con configuraciones predeterminadas más seguras que otros.

Existen innumerables herramientas automatizadas que buscan

vulnerabilidades en sistemas informáticos. Algunas están especializadas en ciertos sistemas operativos o ciertas aplicaciones. Otras son más generalistas. Mayoritariamente, su uso no requiere grandes conocimientos, lo que ha permitido que en los últimos años crezca exponencialmente el número de *script kiddies,* quienes las usan irresponsablemente. Cuando se descubre una vulnerabilidad jugosa, capaz de dar acceso al sistema, con frecuencia se desarrolla una sencilla herramienta especializada en buscar exclusivamente equipos con esa vulnerabilidad. Los gusanos, descritos a continuación, suelen también utilizar esta técnica.

'Malware'

Todo *software* dañino para los sistemas es conocido genéricamente como *malware,* palabra formada por la contracción del término inglés *malicious software.* Suele englobarse dentro del término a virus, gusanos, troyanos, *spyware* y demás artillería que pueda circular por el mundo digital. Este *malware* puede perpetrar una gran variedad de acciones maliciosas: desde robar las contraseñas para acceder al banco hasta enviar *mal-ware* a ordenadores de otros usuarios, pasando por el ataque a servidores de Internet. Y mucho, mucho más.

Durante el año 2008 el incremento en el número de muestras víricas ha sido espectacular. Los antivirus se están enfrentando al mayor desafío desde su creación. En la actualidad, tal y como reconocen algunos fabricantes, se ha perdido la carrera contra los virus. Algunas casas antivirus afirman haber detectado en el último año tantas muestras de *malware* como en la suma de los veinte años anteriores.

Por otro lado, los virus se especializan cada día más. Últimamente están arrasando los troyanos bancarios, diseñados para robar información financiera. Atacan al sistema más usado, Windows, siendo los virus para Mac y Linux prácticamente anecdóticos. Hoy los virus son programas que

llegan de una forma u otra a los ordenadores, normalmente explotando agujeros de seguridad en navegadores, y permiten su control remoto desde el ordenador que los ha distribuido. Su objetivo es bien prosaico: robar dinero.

Repasemos ahora las formas más frecuentes de *malware* a las que se ve expuesto un usuario doméstico típico:

- Virus.
- Gusanos.
- Troyanos.

Virus

Los virus informáticos (denominados así por analogía con los causantes de enfermedades sobre el cuerpo humano) son programas, normalmente dañinos, que se añaden a ficheros ejecutables y tienen la propiedad de ir replicándose a sí mismos por los sistemas y/o ficheros adyacentes. Pueden causar "muertes" de sistemas o simplemente provocar incomodidades que no llegan a más.

Por lo general, necesitan de la participación de los usuarios para propagarse, ya sea a través del intercambio de memorias USB, del envío de mensajes de correo electrónico o de la instalación de programas descargados desde Internet.

Aunque es verdad que existen virus para todas las plataformas, lo cierto es que la inmensa mayoría, en torno al 99%, se circunscriben a la plataforma Windows. No obstante, los usuarios de Linux o Mac tampoco deberían relajarse; aunque el número de virus para estas plataformas es ciertamente escaso, existir, existen.

Gusanos

Los gusanos son pequeños programas que se replican por la Red de forma automática, para lo que se valen de vulnerabilidades de sistemas. A diferencia de los virus, no necesitan que el usuario ejecute un archivo o abra un documento. Como resultado del proceso de copia masivo, los gusanos pueden saturar el ancho de banda de la Red o utilizar todo el espacio de disco de un sistema, por lo que los costes de indisponibilidad que provocan suelen ser considerables.

Troyanos

De igual manera que en la antigua Troya los soldados griegos se escondieron dentro de un supuesto regalo (un caballo de madera), los troyanos son programas aparentemente inofensivos descargados e instalados por el usuario. Además de realizar la función para la que se adquirieron, sin que el usuario se dé cuenta de nada, realizan otras tareas encubiertas, normalmente hostiles. Actualmente, han proliferado desmesuradamente los troyanos bancarios para cometer fraude financiero. Su función consiste en robar las credenciales de acceso a la banca en Internet.

Aunque suelen asociarse al contexto vírico, en realidad los troyanos no comparten ningún rasgo con los virus, ni con los gusanos, ya que ni se autopropagan, característica propia de los gusanos, ni infectan a otros archivos, característica inherente a los virus. Para lograr la colaboración de la víctima y conseguir que el programa sea instalado, los troyanos suelen recurrir a la *ingeniería social,* apelando a la lujuria, a la codicia o al miedo.

INGENIERÍA SOCIAL

La ingeniería social comprende el conjunto de técnicas de cracking destinadas a penetrar en sistemas informáticos, basadas, más que en la pericia técnica, en engañar a la gente para que revele contraseñas y cualquier información que pueda comprometer la seguridad del sistema bajo ataque. Apela a las inclinaciones más profundas de la persona: el miedo, el deseo, la codicia o incluso la bondad.

Hacerse pasar por administrador de un sistema o técnico de un proveedor de servicios

de Internet constituyen estratagemas habituales para conseguir las contraseñas de los usuarios: de su cuenta de correo web, de su cuenta en una tienda virtual, de su cuenta de acceso a Internet... Se atemoriza a la víctima haciéndole creer que ha habido un problema en su cuenta, proporcionando argumentos plausibles ribeteados de jerigonza tecnológica para asegurarse de que no entiende bien qué está pasando, y a continuación se le solicita su contraseña como único medio de restituir el servicio a su funcionamiento normal. O se le incita a llamar a un número telefónico supuestamente para evitar que se le efectúe un cargo en su cuenta de crédito, llamada que le costará una fortuna.

Los virus y troyanos utilizan cada vez con mayor frecuencia técnicas de ingeniería social para camuflarse. Para que la víctima no sospeche, llegan en un mensaje de correo procedente de una dirección tomada de su libreta de direcciones personal, con un título que invita a abrir el mensaje, el cual viaja acompañado de un archivo adjunto o de un enlace a un sitio web donde descargar el archivo ejecutable. El usuario incauto ejecuta el archivo, con los consiguientes resultados desastrosos.

Los troyanos actúan como un servidor instalado en la máquina de la víctima que responde a las peticiones de un cliente remoto, abriendo así un canal de comunicaciones encubierto. Cuando el usuario se conecte a Internet, el troyano avisará a su creador de que la víctima se encuentra en línea. A partir de ese momento, el *ciberatacante* podrá enviar órdenes a través del canal abierto para controlar remotamente el ordenador atacado: robar contraseñas, obtener documentos privados, ejecutar programas, espiar qué hace el usuario en cada momento, suplantarle para enviar mensajes en su nombre, destruir la información de su disco duro, atacar a otros sistemas coordinadamente, ¡lo que quiera!

Los ordenadores comprometidos se denominan *zombies* y normalmente pasan a formar parte de una gran red, la cual puede llegar a contener miles de equipos. Estas redes reciben el nombre de *botnets* y se alquilan para cometer fechorías.

De dónde nos llega el 'malware'

Como queda dicho, el *malware* está compuesto por pequeños programas maliciosos. ¿Cómo pueden llegar a introducirse esos programitas en nuestro ordenador? Depende del tipo de *malware,* pero en líneas generales pueden

señalarse las siguientes vías de entrada o, técnicamente, "vectores de infección":

- Redes de intercambio de archivos (P2P): eMule o BitTorrent han alcanzado una popularidad extraordinaria. Además de música y películas, también es frecuente descargar *software*. Se apunta en algunas estadísticas que al menos el 50% de los programas disponibles para su descarga en redes P2P están infectados. Justicia poética, que dicen algunos.
- Memorias USB: así como en los noventa el medio de intercambio de archivos predilecto era el disquete, hoy en día todo el mundo lleva en el bolsillo su memoria USB. Al ritmo de los tiempos, ahora los virus se contagian pinchando promiscuamente la memoria en cualquier ordenador desconocido previamente infectado. El virus pasa a instalarse en la memoria USB y de ahí se irá propagando a otros sistemas.
- Navegación: muchos virus actuales se introducen en los equipos de las víctimas a través de fallos de seguridad en los navegadores. En este sentido, Internet Explorer posee un palmarés verdaderamente terrorífico. Desgraciadamente, los ojos de los desarrolladores de virus se han vuelto también hacia otros navegadores menos populares, como Mozilla Firefox o Safari. Nadie está a salvo.
- Correo electrónico: los virus todavía se transmiten como archivos adjuntos en mensajes de correo. Claro que lo suelen hacer disimuladamente: en vez de ocultarse en archivos ejecutables como los famosos .EXE, contra los cuales todos los usuarios están advertidos, tienden a ocultarse en archivos ofimáticos, como documentos o presentaciones. O, más disimuladamente aún, en el

correo aparecen hiperenlaces que conducen a sitios web desde los cuales descargar el archivo infeccioso.

- Vulnerabilidades en el sistema operativo y *software:* antes o después salen a la luz nuevos agujeros de seguridad en todos los sistemas operativos y en *software* variado, los cuales pueden permitir a un atacante crear *malware* que los explote maliciosamente.

En los próximos capítulos se ofrecerán consejos para evitar estos vectores de infección.

Fraudes y timos

Internet constituye un importante caldo de cultivo para todo tipo de fraudes, desde los timos tradicionales a los más sofisticados. Entre los que más se han popularizado en los últimos tiempos debido a su elevada rentabilidad se encuentran los ataques de *phishing.*

'Phishing'

El término *phishing* deriva del inglés *fishing,* que significa "pescar". El objetivo del *phishing* consiste en el robo de identidad digital para obtener un lucro indebido. Para mayor concreción, se trata de un *ciberataque* en el cual un atacante (el *phisher*) se hace pasar por una compañía o institución financiera de reconocido prestigio, enviando mensajes de forma masiva (el primer cebo), habitualmente a través del correo electrónico (aunque podrían utilizarse otros canales), como mensajes instantáneos, mensajes en foros o en salas de *chat,* o incluso documentos en Word o en PDF. Sirve cualquier soporte donde aparezca un hiperenlace sobre el que se pueda hacer clic. Los mensajes están dirigidos a potenciales clientes (*phish,* "el pescado") de la organización suplantada, con la esperanza de que muerdan el anzuelo y sean

redirigidos a un sitio web idéntico al original (el segundo cebo) encargado de recolectar la información personal que constituye su identidad digital, típicamente un nombre de usuario y contraseña o los datos de la tarjeta de crédito.

FIGURA 2
Típico mensaje de correo de 'phishing', en el que se promociona el nuevo sistema de seguridad antifraude y se anima a hacer clic sobre el hiperenlace.

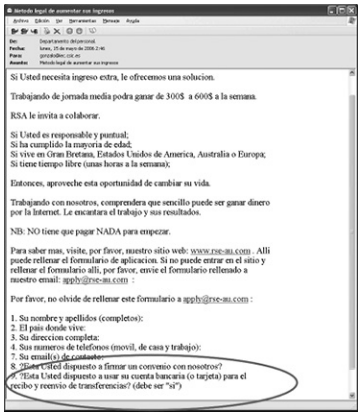
Las estadísticas señalan que alrededor del 5% de los clientes alcanzados muerden el anzuelo, cantidad nada desdeñable si se tiene en cuenta que un *phisher* puede enviar millones de correos al día. Una vez robada la identidad de la víctima, el atacante podrá suplantarla ante el servicio legítimo y abusar de sus servicios.

Otros timos

El correo electrónico se ha erigido en vehículo predilecto de transmisión de timos *(scams)*. Todo usuario del correo recibirá montañas de mensajes que intentan camelarle para que compre algo fraudulento, o participe en alguna operación económica para recuperar el dinero bloqueado de un árabe o un nigeriano. Son viejos timos con nuevo disfraz.

Entre los más peligrosos se cuentan los esquemas tipo “gane dinero desde casa”, cuya finalidad consiste en reclutar *muleros* para coadyuvar en delitos de *phishing*. (Se muestra un ejemplo en la figura 3.) El gancho consiste en una atractiva oferta de trabajo desde casa, para el cual sólo hace falta ser mayor de edad y poco más. Una vez reclutados, se les instruye en su parte del trabajo: deben crear una cuenta bancaria a su nombre en el banco objetivo, en la cual recibirán transferencias periódicas de dinero, que ellos ignoran que procede en realidad de las cuentas comprometidas de las víctimas del *phishing*. El mulero debe transferir este dinero, por ejemplo por medio de un servicio de envío internacional como Western Union o MoneyGram, a una cuenta del estafador en el extranjero, típicamente países de Asia o Europa del Este, quedándose con una comisión de entre un 5% y 10% en concepto de honorarios por el trabajo realizado. Poco sospecha el mulero que, cuando la policía rastree el dinero robado de las cuentas de las víctimas, a quien atrapará será a él y no al estafador, quien habrá volado con el dinero.

FIGURA 3
Típico mensaje de correo para reclutar muleros.


Si Usted necesita ingreso extra, le ofrecemos una solucion.

Trabajando de jornada media podra ganar de 300$ a 600$ a la semana.

RSA le invita a colaborar.

Si Usted es responsable y puntual;
Si ha cumplido la mayoria de edad;
Si vive en Gran Bretana, Estados Unidos de America, Australia o Europa;
Si tiene tiempo libre (unas horas a la semana);

Entonces, aproveche esta oportunidad de cambiar su vida.

Trabajando con nosotros, comprendera que sencillo puede ser ganar dinero por la Internet. Le encantara el trabajo y sus resultados.

NB: NO tiene que pagar NADA para empezar.

Para saber mas, visite, por favor, nuestro sitio web: www.rse-au.com . Alli puede rellenar el formulario de aplicacion. Si no puede entrar en el sitio y rellenar el formulario alli, por favor, envie el formulario rellenado a nuestro email: apply@rse-au.com :

Por favor, no olvide de rellenar este formulario a apply@rse-au.com :

1. Su nombre y apellidos (completos):
2. El pais donde vive:
3. Su direccion completa:
4. Sus numeros de telefonos (movil, de casa y trabajo):
7. Su email(s) de contacto:
8. Sabe Usted dispuesto a firmar un convenio con nosotros?
9. Esta Usted dispuesto a usar su cuenta bancaria (o tarjeta) para el recibo y reenvio de transferencias? (debe ser "si")

En su mayor parte, los timos y fraudes explotan la ingenuidad y buena fe de las víctimas y también su codicia o lujuria. El afán por hacer dinero fácil

o encontrar chollos puede perder a más de uno. Si parece demasiado bueno para ser verdad, no lo dudes, no es verdad. Desconfiar de la palabra “gratis” y de los precios increíbles, huir de compañías con las que no existe ningún otro medio de contacto además de una página web y nunca instalar programas sospechosos para obtener contenidos gratuitos son normas básicas para evitar el fraude.

Otras amenazas

Aunque tendemos a fijarnos exclusivamente en las amenazas externas y llamativas, como *ciberatacantes* y *malware,* lo cierto es que un gran número de incidentes tienen un origen mucho más prosaico:

- Cortes de luz, apagones, irregularidades en el suministro eléctrico: como consecuencia se perderán los datos de la sesión. Si la interrupción es prolongada, el impacto será mucho mayor.
- Averías del *hardware:* en función del dispositivo afectado, el impacto será variable. Por ejemplo, un disco duro estropeado puede suponer la pérdida irremediable de todos los datos, mientras que un ratón averiado se sustituye rápidamente.
- Interrupción de la conexión de red: su impacto será mayor o menor en función del valor que represente para el afectado.
- Fallos de *software:* a veces los programas o sistemas operativos se quedan colgados, provocando la pérdida de los datos de la sesión en curso.
- Errores humanos: se cuentan entre los más temibles. Muchos usuarios de informática son capaces de causar daños irreparables fruto de su ignorancia. También es difícil protegerse frente a ellos.

Resumen

Las amenazas a la información pueden ser externas, procedentes de *ciberatacantes* y *malware,* o pueden ser internas, presentes en nuestra propia casa, como averías y fallos humanos. Sean los incidentes fortuitos o provocados, resulta imprescindible protegerse frente a todos ellos. En los siguientes capítulos se presentarán las herramientas y procesos necesarios para salvaguardar la información.

CAPÍTULO 3

Medidas básicas de seguridad

Durante unas fiestas navideñas observé con curiosidad un gigantesco árbol de Navidad erigido en medio de la plaza de una ciudad, adornado con enormes bolas de diferentes colores. Lo que llamó mi atención fue que día a día iban desapareciendo las bolas: primero las situadas a menor altura, luego las colgadas a alturas superiores, hasta que en una semana el proceso se detuvo alrededor de los dos metros y medio. Se había alcanzado la estatura máxima de la población (con el brazo alargado, claro). Esta anécdota nos enseña importantes lecciones para la seguridad y la gestión del riesgo:

1. Primero se roba el fruto que cuelga más bajo, porque está al alcance de cualquiera, incluso de los niños.
2. El fruto que cuelga a una altura mayor que la estatura máxima de la población queda a salvo, excepto si el ladrón está muy determinado y decide exhibir todos sus recursos: utilizando, por ejemplo, una escalera.
3. Si quieres proteger un fruto, asegúrate de colgarlo a mayor altura que el resto.

Si nuestros equipos domésticos fueran bolas de Navidad, ¿cuáles serían los primeros en sucumbir ante ataques de *ciberdelincuentes* y *malware?* Obviamente, los que no implantan ninguna medida de seguridad, es decir,

los que cuelgan tan bajos en el árbol de Internet que hasta un niño puede alcanzarlos. Nunca perdamos de vista que nuestro ordenador es víctima de ataques indiscriminados que buscan explotar vulnerabilidades conocidas en millones de ordenadores. Nunca seremos el blanco de un ataque determinado dirigido específicamente contra nosotros.

Por tanto, nuestro objetivo debe ser elevar el listón de seguridad a una altura tal que nuestro ordenador quede por encima del nivel medio de los ataques, de manera que exija unos conocimientos avanzados para ser atacado más allá de las técnicas automáticas utilizadas para comprometer ordenadores domésticos. No se trata de volverse invulnerable frente a todo tipo de ataques, vana y cara ilusión, sino de quedar fuera del alcance de ataques de *crackers* y *malware* típicos.

En concreto, se mencionarán las tres medidas de seguridad básicas que no pueden faltar en ningún ordenador doméstico conectado a Internet, las cuales permitirán elevar drásticamente y sin ningún esfuerzo el nivel de seguridad:

- Cortafuegos.
- Antivirus.
- Actualizaciones de seguridad.

Cortafuegos

El cine de Hollywood nos ha enseñado que durante la Edad Media se protegían las poblaciones mediante un alto muro de piedra, con un único punto de entrada custodiado por guardias armados, los cuales examinaban a los que querían entrar o salir y decidían quién pasaba y quién no según las instrucciones que hubieran recibido del señor feudal. En el mundo informático, este tipo de protección se denomina *seguridad perimetral,* en la medida en que busca salvaguardar los equipos informáticos dentro de un

perímetro, como por ejemplo el hogar.

Hoy resulta común encontrar hogares con varios equipos conectados en una pequeña red doméstica, normalmente inalámbrica: ordenadores de sobremesa, portátiles, PDA, videoconsolas, discos duros multimedia, etc. Los cortafuegos, también conocidos como *firewalls,* sin ser la panacea de la seguridad informática, actúan como un muro de protección erigido entre nuestra red interna e Internet. Su misión fundamental consiste en aislar de Internet a los equipos de casa, restringiendo el acceso hacia/desde la red doméstica sólo al tráfico inofensivo.

Del mismo modo que una muralla con su foso no protegía a una ciudad frente a todo tipo de amenazas, tampoco protegerá un cortafuegos frente a todo tipo de ataques informáticos. A pesar de ello, constituye un elemento esencial en la defensa de todo sistema informático, incluidos los domésticos, ya que eleva el listón de las habilidades requeridas por un *ciberatacante* para penetrar en un sistema así defendido. Por así decirlo, hace que nuestra bola de Navidad quede mucho más alta en el árbol.

Una mirada al funcionamiento interno de los cortafuegos

Para entender cómo funcionan los cortafuegos se requiere conocer previamente algunos detalles de los entresijos de las redes de ordenadores. A todos los equipos conectados en una red se les asigna una dirección IP, algo así como el número de teléfono que permite llamar y recibir llamadas. Para que dos ordenadores se comuniquen entre sí, resulta imprescindible que conozcan sus respectivas direcciones IP.

Un ordenador puede ofrecer varios servicios desde Internet:

- Un servidor web ofrece páginas web para navegar por ellas.
- Un servidor de correo ofrece la posibilidad de descargar el correo recibido.

- Un servidor de archivos ofrece archivos para su descarga.

Cada uno de estos servicios se presta en un puerto determinado, identificado por un número fijo. Estos números de puerto funcionan de manera parecida a cuando sintonizamos una emisora de radio o una cadena de televisión: cada estación de radio tiene asignado su propio dial del mismo modo que cada canal de televisión tiene su propia frecuencia. Igualmente, cada servicio de Internet se ofrece en un número de puerto fijo.

Por consiguiente, para conectarse a un servidor habrá que especificar tanto su dirección IP como el puerto en el que se facilita el servicio deseado. Algunos ejemplos de números de puerto típicos son: el 80 para la navegación web (HTTP), el 25 para enviar correos (SMTP), el 110 para leerlos (POP3), el 21 para transmitir archivos (FTP), etc.

Otra característica del tráfico de red es que la información se agrupa en pequeños paquetes de unos y ceros, sin importar si se trata de un documento en PDF, una página web o una fotografía. Es como si quisiéramos mandar un libro a un amigo por correo postal y sólo dispusiéramos de sobres pequeños en los cuales no cabe. Podríamos dividir el libro en pequeños paquetes y mandarlos individualmente, numerados en orden, cada uno en su propio sobre. Podrán llegar en cualquier orden, pero el destinatario será capaz de reordenarlos y recuperar así el libro original.

Del mismo modo, para poder transmitir la información por Internet ésta se secciona en pequeños paquetes, los cuales se envían secuencialmente hasta el receptor, donde son reconstruidos en el orden adecuado. Como si fuera el membrete de una carta, cada paquete de Internet posee una cabecera con la información de la dirección IP y puerto al que va destinado, así como con la dirección IP y puerto de origen. Estas cabeceras constituyen la información fundamental utilizada por los cortafuegos para decidir si un paquete pasa o no pasa.

Veámoslo con un ejemplo. Al solicitar una página a un servidor web, nuestro navegador usará un número de puerto de origen aleatorio, pongamos que el 1100. Este número de puerto se conserva durante toda la sesión de navegación. El navegador establecerá una conexión con el puerto 80 del servidor al que mandará las peticiones, mientras que las respuestas llegarán fragmentadas en paquetes. Gracias a que tras el primer paquete que le llega procedente de nosotros el servidor conoce nuestra dirección IP y nuestro número de puerto, podrá devolvernos las páginas web pedidas durante el curso de la navegación.

Por lo general, un cortafuegos doméstico debería bloquear el acceso a todos los puertos de entrada, es decir, no permitirá que ningún equipo de fuera pueda iniciar una conexión con un equipo de dentro. El único tráfico de entrada permitido es el iniciado desde dentro: como en el ejemplo, al pedir una página web, el cortafuegos permitirá al servidor web devolvernos la página solicitada. Normalmente, esta configuración resulta más que suficiente para equipos domésticos, ya que no es frecuente que ofrezcan servicios al exterior, tales como web, correo, *chat,* etc. Pero existen algunas excepciones como determinados juegos en red, ciertas aplicaciones de videoconferencia o las redes de intercambio de archivos tipo eMule. En todos estos casos será necesario abrir al exterior los puertos correspondientes en el cortafuegos.

Los dos tipos de cortafuegos ideales para el hogar

Los cortafuegos adecuados para el entorno doméstico pueden ser de dos tipos:

1. *Software:* también conocidos como *cortafuegos personales,* son programas que se instalan en todas las máquinas que se desea proteger con ellos. Todos los sistemas operativos en uso hoy en día

en el hogar incorporan un cortafuegos personal que viene activado de manera predeterminada. Este tipo de cortafuegos está presente en las distintas versiones de Windows, tales como XP, Vista, 7; en Mac OS X; y en los distintos sabores de Linux, como el popular Ubuntu. Además de los incorporados de fábrica, existen numerosas empresas de seguridad que ofrecen cortafuegos personales semejantes, normalmente con superiores prestaciones y funciones adicionales. Se comercializan bien como productos independientes o bien formando parte de una suite de seguridad. Una buena noticia es que existen cortafuegos personales de gran calidad gratuitos para el usuario doméstico, como ZoneAlarm, COMODO Internet Security o Sunbelt Personal Firewall y, por supuesto, otros muchos más de pago.

2. *Hardware:* se suelen instalar en el punto de conexión a Internet y protegen a todos los equipos detrás del mismo. Los *routers* ADSL o cable proporcionados por la compañía de acceso a Internet vienen equipados con un cortafuegos. La configuración predeterminada estándar deniega el acceso desde el exterior a todo tipo de tráfico, obligando a abrir puertos en caso de ser requerido. Se trata de una resolución conservadora y, por tanto, adecuada. Sin importar cuántos equipos convivan dentro del hogar, todo el tráfico que generen se verá forzado a pasar por el cortafuegos, como si de un puente levadizo se tratase, con lo que todos ellos se verán convenientemente protegidos. Existen cortafuegos *hardware* de grandes prestaciones, pero tanto sus capacidades como su precio exceden las necesidades de un hogar común.

Estrategia de uso de cortafuegos en el hogar

Ambos tipos de cortafuegos, *software* y *hardware,* no son mutuamente excluyentes, sino que pueden y deben coexistir para mayor seguridad.

Si la conexión a Internet se realiza a través de un *router* ADSL o cable, entonces éste bloqueará todo tráfico dirigido hacia el interior. Conviene consultar el manual de instrucciones del *router* o pedir asesoramiento a la compañía de telecomunicaciones que presta el servicio de Internet para aprender cómo se configura el filtrado de paquetes y para aprender a abrir y cerrar puertos en caso de que se necesite.

Para complementar esta primera barrera de protección, conviene además tener instalado un cortafuegos personal en todo equipo capaz de incorporar uno, como los PC de sobremesa o portátiles. El motivo es que el *router* típicamente se limita a bloquear el tráfico de entrada, pero no el de salida, mientras que los cortafuegos personales pueden ayudar a bloquear también el tráfico de salida generado por la actividad malintencionada del *malware.* Estos cortafuegos pueden detectar y bloquear los intentos de conexión por parte de troyanos y gusanos hacia el mundo exterior y, en general, pararles los pies a los *ciberatacantes*.

Se recomienda activar siempre el que acompaña al sistema operativo o, para los espíritus intrépidos, probar incluso alguno de los gratuitos. Son fáciles de configurar, consumen escasos recursos e idealmente deben dar poco la lata. No hay nada más incómodo que pequeñas ventanas de alerta que nos detienen a cada paso solicitando permiso para cualquier acción. Se trata por tanto de encontrar el equilibrio entre comodidad y seguridad.

INTERNET NO ME FUNCIONA DESDE QUE TENGO EL CORTAFUEGOS

Debemos tener en cuenta que un cortafuegos configurado de forma excesivamente restrictiva puede impedir que muchos programas se conecten a Internet cuando los servidores ofrecen su servicio en números de puerto no estándar o cuando queremos que un equipo de nuestra red actúe como servidor.

Supongamos que hemos permitido hacia el exterior sólo la conexión al puerto 80 para navegar por Internet. Si un servidor se mantiene a la escucha en otro puerto, por ejemplo el 8080, entonces no podremos ver sus páginas. Habrá que abrir ese puerto

de salida en los cortafuegos, software y hardware, y una vez terminada la sesión de navegación, volver a cerrarlo.
Muchos usuarios que usan programas para compartir archivos como eMule o juegos en red se encuentran con que no les funcionan. El problema radica en que el cortafuegos bloquea el acceso desde el exterior. Habrá que abrir los puertos de entrada requeridos en los cortafuegos y dejarlos abiertos mientras se sigan usando esos programas. Debe consultarse el manual del router para aprender a abrir estos puertos y para configurar una característica llamada NAT, la cual permite que el router sepa a qué equipo de entre todos los de la red interna van dirigidos los paquetes procedentes desde el exterior.
En general, más vale pasarse de restrictivo que de permisivo. Siempre resulta más seguro empezar cerrándolo todo e ir abriendo poco a poco lo que se va necesitando que actuar al revés, dejándolo todo abierto, porque entonces quedarán grandes agujeros sin tapar.

Antivirus

La mejor línea de defensa contra el *malware* la constituye un buen antivirus. Este tipo de *software* ha ido evolucionando en los últimos años hasta incluir diversos componentes de seguridad más allá de la lucha contra los virus. Actualmente, los antivirus suelen comprender además del antivirus propiamente dicho herramientas *antispyware,* filtrado *antispam*, protección contra *phishing,* control de contenidos, corta-fuegos personal, etc. De hecho, se comercializan muchos productos no como simples *antivirus* sino como *suites de se-guridad.*

Sin perder de vista la definición de *malware* vista en el capítulo 2, el *software* antivirus debería protegernos como mínimo de virus, gusanos y troyanos. El resto de protecciones pueden o no estar presentes, pero no se considerarán en este capítulo, sino en el siguiente, ya que no son tan graves como el *malware.*

Cómo funcionan los antivirus

Todo programa antivirus incluye un *motor de escaneo,* encargado de buscar *malware* en el disco duro del ordenador o en el tráfico procedente de Internet. Para saber qué es *malware* y qué no, los antivirus cuentan con una

inmensa lista de *firmas*. Cada ejemplar de virus posee una firma única, algo así como su huella dactilar que lo identifica y distingue de los demás. El antivirus busca en cada archivo escaneado coincidencias con alguna firma de la lista y, en caso afirmativo, la muestra se etiqueta como virus.

Dado que se crean nuevos virus cada día, es necesario mantener las listas de firmas constantemente actualizadas. A pesar del titánico esfuerzo realizado por las casas antivirus, el ritmo de creación de *malware* es tan fabuloso que resulta imposible crear una firma para cada virus existente. Por este motivo, los antivirus también utilizan *heurísticas:* un proceso por el cual la información acerca de virus ya conocidos permite identificar como *malware* el comportamiento sospechoso de ciertos programas a pesar de no poseer una firma específica para ellos.

El problema de las heurísticas y otras formas de detección de virus desconocidos es que originan muchos falsos positivos. Se llama *falso positivo* a una falsa alarma, es decir, cuando el antivirus etiqueta como *malware* a un fichero inocente, igual que en el cuento, cuando Pedrito grita que viene el lobo, pero no es así. El inconveniente de los falsos positivos es que si crece su número se termina perdiendo confianza en la capacidad de detección del antivirus, como le ocurrió a Pedrito ante los aldeanos.

Los programas antivirus efectúan el escaneo de archivos en busca de *malware* de varias formas:

- Al vuelo o en tiempo real: constituye la principal barrera contra el *malware,* ya que el escaneo se está realizando continuamente entre bambalinas sin que nosotros nos percatemos de nada cada vez que abrimos un archivo o usamos Internet para navegar o abrir un adjunto recibido por correo electrónico.
- Planificada: ayuda a comprobar que no se hayan colado virus en el ordenador. Se configura el programa antivirus para que

periódicamente escanee todo el disco duro en busca de *malware* que pudiera habérsele pasado al escaneo en tiempo real, por ejemplo porque todavía no estaba actualizada su firma. Suele planificarse como mínimo una vez a la semana. Debido a que puede exigir mucho tiempo y consumo de recursos, mejor programarla para la noche, a horas en que no se espera utilizar el ordenador.

- Manual: es semejante a la planificada, pero iniciada a voluntad por el usuario. El escaneo puede extenderse a todo el disco o sólo a una parte: un directorio o incluso un único archivo.

'Software' de antivirus siempre al día

El *software* antivirus debe mantenerse siempre actualizado y funcionando. Un antivirus cuyas firmas no se actualizan vale tanto como no tener ninguno. La mayoría de ordenadores recién adquiridos vienen con un antivirus preinstalado, normalmente con una suscripción de alrededor de 90 días, suficiente para que cuando caduque nos hayamos acostumbrado a él y no podamos vivir sin su compañía. Cuando expira la licencia, el antivirus puede continuar operativo, pero si no se actualizan las firmas, ya no vale para nada. ¡Hay que actualizar las firmas!

Dado el frenético ritmo de crecimiento de virus, las actualizaciones de firmas deberían realizarse diariamente. A la hora de elegir un producto antivirus prestaremos especial atención a la facilidad y frecuencia de actualización. Los hay con actualizaciones automáticas programadas cada pocas horas.

Cómo elegir un antivirus

Existen varios productos totalmente gratuitos y que actualizan automáticamente sus firmas, lo cual los convierte en un excelente punto de

partida para familiarizarse con este tipo de *software* si no se quiere gastar dinero: AVG Anti-Virus Free Edition, BitDefender 10 Free Edition, Avira AntiVir Personal Edition, avast! 4 Home Edition, Malwarebytes' Anti-Malware, Panda Cloud Antivirus, Microsoft Security Essentials.

También existen versiones en línea de los antivirus, como las que ofrecen Panda, Trend Micro, McAfee, Norton y otros.

Por último, existe una larga lista de productos antivirus de pago. La recomendación es utilizar siempre el producto comercial de una casa de reconocido prestigio. Del mismo modo que si vas a escalar no comprarías una cuerda barata de segunda mano en un mercado callejero porque está en juego tu vida, si valoras tus datos y la seguridad de tu información, no renunciarás a un buen antivirus. Los precios para el mercado residencial son totalmente asequibles.

Para el usuario doméstico, la característica más importante que debe poseer un antivirus por encima de cualquier otra es su facilidad de uso y configuración. Otro punto de interés a tener en cuenta es el consumo de recursos. El hecho de tener un programa que está escaneando continuamente el disco duro y analizando el comportamiento de los programas puede ralentizar considerablemente la velocidad del ordenador.

No hay que olvidar el tipo de servicio posventa prestado por el fabricante. Si de algo puedes estar seguro es de que antes o después tendrás un problema causado por *malware.* Aquí es donde un buen soporte al cliente vale su precio en oro. De hecho, un buen antivirus vale más que su precio en oro. Desde el momento en que detenga el primer virus ya habrá devuelto la inversión.

Por último, una nota de cautela. En palabras de los técnicos de VirusTotal, servicio *on line* de análisis de archivos sospechosos que permite detectar virus, gusanos, troyanos y *malware* en general: "No existe solución

en el mundo que pueda ofrecer un 100% de efectividad en el reconocimiento de virus y *malware* en general. Si le ofrecen un producto con el 100% de efectividad, está siendo víctima de publicidad falsa".

Actualizaciones de seguridad

Cuando era niño, si me hacía un agujero en un pantalón, mi madre le ponía un parche y yo seguía usándolo. Con el tiempo, parche a parche, mis pantalones favoritos, de los cuales no quería desprenderme, terminaban exhibiendo rodilleras, culeras y remiendos en otros rincones.

Continuamente se descubren fallos de seguridad en los sistemas operativos, es decir, agujeros por los que pueden colarse los *ciberatacantes* y el *malware*. Los fabricantes de *software* se esfuerzan por mantener sus productos actualizados, y publican parches que corrijan los errores de seguridad detectados. A pesar de la extensa cobertura mediática de los fallos en Windows, en todas las casas cuecen habas: en todos los sistemas operativos, incluidos los Mac y los derivados de Linux, continuamente se descubren agujeros de seguridad serios. Por si fuera poco, en los distintos programas y aplicaciones, desde los distintos navegadores hasta las aplicaciones ofimáticas o los productos de Adobe, aparecen de tiempo en tiempo graves vulnerabilidades que pueden ser explotadas por atacantes para tomar un control total de las víctimas afectadas.

Los distintos fabricantes publican los parches de manera periódica o en respuesta a grandes problemas de seguridad: son como los parches para ir planchando sobre el pantalón cada vez que aparece un nuevo agujero. Por lo general, al poco tiempo de publicarse un parche, y a veces incluso antes de que se publique, el agujero que soluciona será explotado por *ciberatacantes* o *malware* para comprometer los equipos que no lo hayan parcheado. Por tanto, es fundamental anticiparse a los ataques y parchear cuanto antes.

Con el fin de facilitar la vida a los usuarios, los sistemas operativos, ya

sea Windows, Mac o Linux, permiten configurar la búsqueda, descarga e instalación automáticas de actualizaciones de seguridad. Estar al día constituye un requisito fundamental para conservar una oportunidad de sobrevivir en el mundo rápidamente cambiante de Internet. Al igual que un pantalón puede estar nuevo hoy, pero con el uso dejará de estarlo mañana, que nuestros equipos estén seguros en un momento dado no significa que lo sigan estando en el futuro. La seguridad exige un esfuerzo continuo de actualización.

Del mismo modo, gran parte del *software* que se ejecuta sobre el sistema operativo ofrece formas sencillas de actualizarse: navegadores, clientes de correo, productos de Adobe, el motor de Java, reproductores multimedia, etc.

Debemos consultar la ayuda de nuestro sistema operativo y de los programas que utilizamos para informarnos acerca de la política de actualizaciones del fabricante, de si es posible configurar actualizaciones automáticas y cómo hacerlo. Mejor no depender de nuestra diligencia, sino que nuestro *software* se actualice solo en cuanto el fabricante publique nuevos parches.

Resumen

¿Quieres que tu ordenador esté a salvo de *ciberatacantes,* virus, gusanos y troyanos? Muy fácil: no lo conectes a Internet ni instales *software* ni cargues ningún tipo de archivo desde una memoria USB o desde un CD. Sólo un ordenador completamente aislado del mundo exterior puede estar seguro y, aun así, no me atrevería a poner la mano en el fuego. Pero ¡qué aburrido! Un ordenador así no nos resultaría de mucha utilidad.

Afortunadamente, podemos alcanzar un término medio: cortafuegos, antivirus y actualizaciones de seguridad aportan protección suficiente para conectar nuestros equipos a Internet con confianza. Estas tres medidas de

seguridad son absolutamente imprescindibles y deben ser implantadas por todo tipo de usuario.

CAPÍTULO 4

Medidas avanzadas de seguridad

Los cortafuegos, los antivirus y las actualizaciones son las medidas de seguridad que no pueden faltar en ningún hogar; sin ellas no duraríamos más de unos segundos conectados a Internet. Pero existen otras muchas amenazas y peligros además de los *ciberatacantes* y el *malware.* En función del uso que hagamos del ordenador y de qué activos de información valoremos más, deberemos implantar algunas o todas las medidas que serán tratadas en este capítulo y que hemos agrupado en tres categorías:

- Contenidos molestos o inadecuados, como el *spam,* el *spyware* y la pornografía.
- Fallos de *software* y *hardware,* tanto de los equipos informáticos como de la alimentación eléctrica o de la conexión a Internet.
- Protección de la privacidad y del anonimato, tanto frente al mundo exterior como frente a otros miembros de la familia.

Contenidos molestos o inadecuados

Correo basura que inunda nuestros buzones con ofertas de productos y servicios en los que no estamos interesados, programas espía que recaban información sobre nuestros hábitos de navegación, contenidos violentos o pornográficos inapropiados para menores… Internet no es Disneylandia. En un espacio virtual en el que no falta de nada y todo se ve representado, también es de esperar encontrarse con reflejos del mundo real que no nos

hacen tanta gracia. Veamos qué amenazas nos acechan y cómo protegernos frente a ellas.

La lucha contra el correo basura

Algo que da mucha rabia es llegar al portal de casa, abrir el buzón y encontrárselo rebosante de folletos y propaganda. En vacaciones, después de una ausencia prolongada, el buzón puede llegar a saturarse con publicidad de tal manera que el cartero no pueda ni introducir las cartas personales dirigidas específicamente a nosotros.

El correo basura o *spam* aplica el mismo concepto al mundo digital, pero con una importante diferencia: la economía de escala. Enviar correo publicitario en papel cuesta dinero y su difusión es limitada. Sin embargo, el *spam* no se topa con esas barreras. Lo mismo da enviar un correo que un millón; mientras se disponga de direcciones de correo suficientes, el resto es apretar un botón. Nadie que posea una dirección de correo electrónico podrá escapar por mucho tiempo de sus implacables garras.

El correo basura es indeseable

Por muchos motivos:

- El correo basura, como su propio nombre indica, es basura. ¿Y a quién le interesa recibir basura en su buzón? La inmensa mayoría de los correos basura indiscriminadamente enviados por la Red anuncian géneros sin el más mínimo valor, engañosos y más o menos fraudulentos.
- Puede llegar a saturar nuestro buzón electrónico hasta el punto de que tiremos junto con la basura correos legítimos.
- Nos hace perder tiempo separando el grano de la paja, nos hace perder ancho de banda mientras lo descargamos y nos hace perder espacio en disco una vez descargado.

- Es vehículo de virus, *phishing,* pornografía y timos. Si algún mensaje posee un asunto atractivo podríamos sentir la tentación de leerlo y, lo que es peor, seguir sus instrucciones para recoger el premio de un supuesto sorteo o para ganar dinero fácil desde casa.

Filtrado del correo basura

Admitámoslo: todo usuario habitual del correo electrónico ha sido o será muy pronto una víctima más del *spam.* No podemos evitar que nos envíen correo basura a nuestra dirección, pero sí podemos intentar no verlo, de forma que nos perturbe lo menos posible. ¿Cómo? Instalando algún *software antispam.*

Si somos usuarios de servicios de correo web como Yahoo!, Hotmail o Gmail, no debemos preocuparnos, ya que ellos se encargan de filtrar nuestro correo.

Sin embargo, si descargamos el correo directamente a nuestro ordenador usando programas tan populares como Microsoft Outlook Express o Mozilla Thunderbird, entonces necesitaremos protección contra el *spam.* Lo primero de todo es informarse de si nuestro programa para leer el correo incorpora algún tipo de filtro o bloqueo del *spam.* Por seguir con los ejemplos citados, Outlook Express no incorpora filtros de manera nativa, mientras que Thunderbird sí que trae un sofisticado sistema de lucha contra el correo basura.

Si nuestro lector de correo no incorpora protección y nos llega mucho *spam,* podemos pasarnos a otro lector que sí la incorpore. Por ejemplo, los usuarios del veterano Outlook Express pueden pasarse a Windows Live Mail, que sí incorpora protección *antispam.* La otra posibilidad consiste en instalar un programa *antispam* de terceros. Existen productos gratuitos, como G-Lock SpamCombat, SPAMfighter y Spamihilator. También existen

suites de seguridad de casas antivirus que entre sus muchas protecciones ofrecen una contra el *spam.*

¿De dónde sacan los 'spammers' nuestra dirección de correo?

Utilizan todo tipo de fuentes:

- Recolección en sitios web: nada más fácil que escribir un programa que se dedique a buscar direcciones de correo en páginas web.
- Fuerza bruta sobre diccionarios: también pueden crearse combinaciones de palabras y de nombres y apellidos para intentar adivinar direcciones reales.
- Listas de correo comerciales: por cinco euros puede comprarse un DVD con miles de direcciones de correo.
- Concursos y promociones: cuidado con dónde entregas tu dirección de correo. Desconfía de sitios de dudosa apariencia, pues lo más probable es que la vendan.
- Copias de carbón: a veces recibo correos con chistes o bulos donde tengo que desplazar varias pantallas llenas de direcciones de correo hasta llegar al mensaje en sí. Cuando mandas archivos a varias personas y las pones en copia, nunca uses la copia carbón (CC), ya que todas ellas verán las direcciones de los demás. En su lugar, utiliza la copia de carbón oculta (CCO). Todos los programas de correo la incorporan. Consulta su ayuda para aprender a usarla.

Prevención: cómo limitar el correo basura

Dicen que prevenir es curar. Siguiendo estos consejos se conseguirá minimizar la cantidad de *spam* enviado a nuestra dirección de correo:

- Por si hace falta decirlo, ¡nunca respondas! No abras el correo de *spam,* no respondas y, por supuesto, no compres nada ni te creas una sola palabra.
- Crea muchas direcciones de correo web diferentes y utiliza cada una para distintas funciones: una para publicar en foros, otra para suscribirte a listas de distribución, otra para cuando te la pidan al registrarte para obtener ciertos servicios, otra para dar a la gente que conoces en el *chat,* etc. De esta forma, si alguna dirección se ve infestada por el *spam*, simplemente te olvidas de ella, creas otra nueva y a correr.
- Cuando alguien a quien no quieras revelar tu dirección de correo deba enviarte un mensaje, utiliza un servicio como Mailinator. No permite enviar correo, sólo recibirlo. No requiere darse de alta. Basta con inventar cualquier dirección del tipo "loquesea@mailinator.com" y podrás consultar en su sitio web los mensajes recibidos en ese buzón.
- Evita escribir en páginas web tu dirección de correo personal, la que no quieres que caiga en manos de *spammers.* En su lugar, puedes utilizar una imagen con el texto de tu dirección o recurrir a trucos como escribirla con todas las letras: *fulano arroba gmail punto com.*

A salvo de 'software' espía en el ordenador

¿Cómo es posible que haya cadenas de televisión privadas que difunden sus contenidos en abierto sin cobrar a los telespectadores? ¿Por qué existen periódicos gratuitos como el *20 minutos*? La respuesta es bien sencilla: gracias a la publicidad.

'Adware'

En Internet las cosas no funcionan de forma muy distinta. Si una empresa ofrece algo gratuitamente, debe financiarse por otro lado. En concreto, el *software* que se financia a base de publicidad recibe el nombre de *adware* (del inglés *ad,* "anuncio"). Los anuncios pueden aparecer en forma de ventanas emergentes *(popups)* o de pequeños carteles *(banners)*. Hasta ahí, todo sería como en la radio o en las vallas publicitarias y no habría mayores problemas. Ahora bien, un programa instalado en un ordenador puede monitorizar a qué sitios web nos conectamos, a qué usos dedicamos nuestro equipo y retransmitir toda esta información a la compañía para que nos envíe publicidad personalizada.

Claro que ¿quién querría instalar un programa así? Irónicamente, todos lo hacemos. Seamos sinceros, ¿alguien ha leído alguna vez de pe a pa la licencia de un programa antes de instalarlo? Al hacer clic en el botón "Acepto", consentimos, sin saberlo, este comportamiento, aunque no porque no se nos haya informado.

Incluso aunque no nos preocupe lo más mínimo nuestra privacidad, no hay que perder de vista el impacto que este tipo de *software* puede tener en el rendimiento del equipo, ya que está funcionando continuamente en el trasfondo recopilando información sobre nuestros hábitos.

'Spyware'

Si bien el *adware* bordea la frontera de la legalidad, ya que nos avisa con antelación sobre cómo se comportará, el *software* espía o *spyware* da un paso más allá, traspasándola descaradamente. Más cercano a los troyanos que al *adware,* el *spyware* busca compilar detallados perfiles de navegación, gustos, hábitos, preferencias y demás información personal sobre los consumidores, todo ello de forma secreta, sin el conocimiento ni consentimiento del usuario. A intervalos de tiempo retransmite la información recabada, igualmente de manera sigilosa. Algunas formas de

spyware pueden llegar a registrar las pulsaciones de teclado con el fin de capturar nombres de usuario y contraseñas, números de tarjeta de crédito, etc., actividades claramente delictivas.

Limpieza de 'adware' y 'spyware'

La mayoría de suites de seguridad incluyen herramientas para limpiar al ordenador de esta plaga. De hecho, según muchas definiciones de *malware,* el *spyware* conforma otra de sus categorías, junto a los virus, gusanos y troyanos, por lo que la mayoría de antivirus lo detectan y eliminan.

Existen además numerosas herramientas gratuitas creadas específicamente para eliminar *adware*/*spyware* del ordenador. Entre ellas destacan por su solera y eficacia Ad-Aware, Spybot S&D y Windows Defender.

Prevención: cómo limitar el 'adware/spyware'

Una vez más, debemos apelar al sentido común. Algunos usuarios domésticos son instaladores compulsivos: en cuanto ven durante sus correrías por Internet un *software* que puede descargarse e instalarse, ahí que se lanzan.

Debemos ser cuidadosos con lo que instalamos, leer las licencias, analizar el programa antes de instalarlo con nuestro antivirus o con VirusTotal, no instalar ningún programa descargado de redes de intercambio de archivos como eMule, utilizar cortafuegos personales que filtren el tráfico de salida para que nos avisen de intentos subrepticios de conexión por parte del *adware*/*spyware,* evitar los sitios web de contenidos dudosos y nunca instalar ningún programa especial para visualizar contenidos en formatos extraños.

Contenidos bajo control

Si eres padre de familia, te preocupará saber por dónde navegan tus niños,

qué contenidos ven y si son convenientes para ellos. Existe una amplia oferta de productos *niñera* o de *control parental,* cuya misión consiste en filtrar los contenidos considerados inadecuados por los padres. Estos programas normalmente se instalan en el ordenador cuya navegación se desea proteger.

Por lo general, se suelen usar dos aproximaciones para resolver el problema del filtrado de contenido inadecuado: o bien el bloqueo de palabras clave perniciosas, que hacen suponer la presencia gráfica o textual de material desaconsejable en una página web, o bien el listado de sitios web con contenido recomendable y de sitios web con contenido reprobable, prohibiéndose el acceso a estos últimos.

Ahora bien, no vayamos a creer que son la panacea. Presentan varios problemas que debemos sopesar si estamos pensando adquirir uno:

- Ninguno es eficaz cien por cien y a menudo se bloquean páginas que nada tienen de nocivas pero que a lo mejor incluyen una palabra desafortunada.
- A veces un adulto no tiene control sobre los filtros y listas, sino que es la empresa que comercializa el producto la que los configura.
- Las listas de sitios web cambian diariamente, lo que exige actualizarlas manualmente o descargar listas del fabricante, a menudo pagando.
- El manejo y configuración de algunos productos resulta complejo.
- Los niños y estudiantes avispados terminan por aprender cómo saltarse estas protecciones.

Algunos sistemas operativos, como Windows Vista, Windows 7 o Mac OS X Leopard, incorporan controles parentales para supervisar y controlar

el tiempo que pasan tus hijos en el ordenador, los sitios que visitan, qué instalan y descargan y con quién "chatean". Si tu ordenador tiene alguno de esos sistemas operativos, consulta la ayuda para aprender a configurar el control parental.

Existen además paquetes de *software* niñera comerciales creados por terceros. En España el más popular es Optenet WebFilter PC. Por su lado, Microsoft ofrece gratuitamente el producto Windows Protección Infantil, con el que podrás limitar las búsquedas, bloquear o permitir sitios web, decidir con quién pueden comunicarse tus hijos cuando utilizan Windows Live Messenger, Hotmail o Spaces y supervisar los sitios web que visitan.

Otro enfoque completamente diferente consiste en que el proveedor de acceso a Internet filtre directamente los contenidos. De esta manera, no es necesario instalar ningún *software* en los equipos que se utilizan para salir a Internet. Algunos proveedores como Telefónica, ONO u Orange ofrecen a sus clientes de banda ancha la posibilidad de contratar servicios de filtrado de acceso a Internet, los cuales permiten limitar los accesos a páginas web y la descarga de determinados tipos de archivos. No requiere la instalación de ninguna aplicación para el funcionamiento del servicio, lo que facilita que el mantenimiento y actualización lo realice el proveedor en sus propios servidores, sin molestias para el usuario final.

Más adelante, en el capítulo 6, se ofrecerán más consejos para proteger a los menores en Internet.

Fallos de 'software' y 'hardware'

Uno de los pilares de la seguridad de la información consiste en garantizar la disponibilidad, es decir, que los datos permanezcan accesibles sin interrupciones cuando y donde se los necesite. La disponibilidad exige que se implanten una serie de medidas para asegurar un nivel razonable de rendimiento, una gestión rápida y eficiente de las interrupciones,

proporcionar redundancia en caso de fallos, mantener copias de seguridad actualizadas y evitar la pérdida o destrucción de datos.

En un sistema informático son muchas las cosas que pueden marchar mal: puede irse la luz, un disco duro puede dejar de funcionar, un *router* puede estropearse, se puede perder la conectividad exterior… y quién sabe qué más. Hay que estar prevenido para el desastre.

Datos siempre a salvo

Cuando los archivos han sido destruidos y la información ha desaparecido, sólo existe una solución para retornar a la normalidad: tirar de *backup,* esto es, acudir a las copias de respaldo y restaurar el sistema al estado en que se encontraba cuando se realizó la última copia de seguridad. El respaldo de archivos resulta esencial para asegurar la integridad y disponibilidad de los datos. La conservación de copias de seguridad de la información valiosa constituye nuestro seguro de vida en caso de que el desastre llame a la puerta.

A continuación responderemos a las preguntas más típicas que todo usuario se plantea a la hora de gestionar las copias de seguridad.

¿De qué datos debo hacer copias de seguridad?

En todo equipo existen dos tipos de información bien diferenciados:

- Información de sistema: se trata de los archivos del sistema operativo y de todo el *software* instalado.
- Información de usuario: se refiere a los datos generados por los usuarios: documentos de ofimática, fotos, vídeos, planos, dibujos, correos, etc.

La pérdida del primer tipo de información no resulta excesivamente trágica: para volver a la situación original basta con reinstalar el sistema

operativo y el *software.* En el peor de los casos, no se pierde más que tiempo.

Sin embargo, resulta crucial mantener copias de seguridad de la información de usuario. Su pérdida sí que puede representar un desastre. Por lo tanto, como mínimo deberá hacerse siempre una copia de seguridad de los datos personales.

De hecho, una buena práctica consiste en utilizar siempre al menos dos discos duros, de manera que el sistema operativo y todo el *software* se instalen en uno, y los datos de usuario y de trabajo en otro. Así se facilita el proceso de copias de seguridad y se ofrece cierta protección frente a fallos de *hardware:* si se muere el disco con el *software,* no perderemos nuestros datos.

¿Cómo copio los datos?

La forma fácil y rápida consiste en copiar los archivos arrastrando sin más de un medio a otro. Para facilitar las cosas, conviene separar muy bien los distintos contenidos: los vídeos en una carpeta, las fotos en otra, la música en otra, los documentos en otra, y así sucesivamente, cada tipo de contenido en su carpeta correspondiente. Se recomienda también, si es posible, utilizar un disco físico para los datos y otro para los programas y el sistema operativo.

Los sistemas operativos más empleados en el hogar, como distintos tipos de Windows, de Mac o de Linux, incorporan herramientas nativas para la realización de copias de seguridad. Se recomienda utilizar estas herramientas frente a la mera copia, porque aportan importantes ventajas, como por ejemplo el control de qué archivos han sido ya copiados y cuáles no. Consulta la ayuda de tu sistema operativo para informarte sobre cómo usar sus herramientas para copias de seguridad.

¿En qué tipo de soporte los almaceno?

En entornos domésticos suele recurrirse a medios de almacenamiento económicos y fáciles de usar:

- El más popular y barato es el DVD (R y RW), con un dilatado tiempo de vida, superior a los treinta años.
- Otro medio muy usado en los hogares es el disco duro externo. Son normales ya los discos con capacidades de 500 GB y hasta 1 TB, a precios muy razonables.
- Gracias al aumento progresivo del ancho de banda, también se están popularizando los almacenamientos en línea, es decir, las copias de seguridad remotas. Servicios como Banckup o Mast Backup Online ofrecen copia remota de datos, vía Internet, con máximas garantías de seguridad y confidencialidad, para todas las plataformas y planes muy económicos para entornos domésticos. Una ventaja añadida de estos servicios es que se puede acceder a las copias desde cualquier lugar. La mayoría de empresas de *hosting* de Internet ofrecen este servicio, al igual que los suministradores de conexión a Internet. Consulta a tu proveedor de servicios de Internet.

¿Con qué frecuencia debo hacer copias de seguridad?

Podemos dividir nuestros archivos en dos categorías:

- Los que van cambiando con el tiempo: documentos de trabajo en Excel o Word, bases de datos personales en Access, proyectos del tipo que sea en los que estamos trabajando durante meses, etc.
- Los que no cambian: fotos, vídeos, música, películas, etc.

Ambos tipos de datos requieren tratamientos distintos. Los que no

cambian pueden almacenarse definitivamente en DVD-R (los DVD que pueden grabarse una sola vez), cuidadosamente etiquetados para facilitar su posterior recuperación; mientras que para los que van cambiando a lo largo del tiempo pueden utilizarse DVD-RW (los DVD que pueden regrabarse múltiples veces), discos duros portátiles o almacenamiento remoto.

Dado que las copias de seguridad consumen espacio y cuestan dinero, no puede almacenarse un número ilimitado de ellas. En algún momento habrá que reutilizar los DVD-RW o los discos externos. La importancia de los datos y la velocidad de cambio de los mismos dictarán la frecuencia con que se graban y el tiempo que se conservan antes de ser sobrescritos. Cada cual tendrá que analizar estos parámetros y decidirse por los tiempos óptimos para él y sus datos.

¿Dónde guardo las copias de seguridad?

Conviene tenerlas a mano, por si hacen falta. Es importante el correcto etiquetado de los DVD o de los discos y la buena organización. ¡Rebuscar entre docenas de DVD sin ningún rótulo es muy aburrido!

Deben identificarse todos los datos que se consideren vitales y hacer otra copia de seguridad extra para almacenarla en un lugar lo más alejado posible del hogar. De esta manera, si ocurre un desastre serio en el hogar, no afectará también a las copias. En este sentido, las copias remotas vía Internet resultan ideales.

¿Quién las hace?

Conviene nombrar a un responsable en casa que se ocupe de hacer las copias, etiquetarlas, almacenarlas y restaurarlas en caso de necesidad. Si esta persona va a utilizar programas de copia de seguridad, debería familiarizarse antes con su manejo para que luego no surjan sorpresas. En especial, debería hacer ensayos de restauración de datos, porque no siempre se obtienen los resultados esperados.

A salvo de cortes de luz

Por desgracia, ninguna compañía eléctrica garantiza un suministro eléctrico estable 24 horas al día, 7 días a la semana. Por si los problemas de las operadoras de energía no fueran suficientes, algunos pequeños incidentes como fuertes lluvias, calor excesivo o cuadros eléctricos mal dimensionados pueden provocar apagones cuando menos se los espera. Es muy frecuente encontrarse con estos apagones en verano, cuando los sistemas de aire acondicionado sobrecargan las líneas de energía y hacen saltar el limitador. Sea cual sea la causa, de lo que puedes estar seguro es de que antes o después, y generalmente en el peor momento, se producirá alguna anomalía en el suministro.

Protegerse contra estas eventualidades requiere instaurar una estrategia de protección del suministro eléctrico:

- Protectores de sobretensión: como mínimo, una instalación eléctrica doméstica debe contar con una regleta de enchufes con interruptor que incorpore un circuito protector contra sobretensiones con el fin de proporcionar estabilidad eléctrica a los equipos conectados a dicha base. Su precio es muy económico, por lo que todo tipo de usuario puede permitírselo. En mi casa hubo un pico de tensión que se cargó las fuentes de alimentación de todo lo que no estaba enchufado a una de esas regletas con varios enchufes y su interruptor rojo. Si viene una sobretensión, se funde la regleta y no los equipos que tenemos conectados a ella.
- Sistemas de alimentación ininterrumpida: los sistemas de alimentación ininterrumpida (SAI o UPS en inglés) permiten que un equipo informático continúe operando sin suministro eléctrico durante un tiempo que suele oscilar entre cinco minutos y dos

horas, en función del SAI y del consumo de los equipos protegidos. Su finalidad es impedir que el trabajo se pierda si se produce un corte de luz, ya que su autonomía es muy limitada y sólo alcanza para guardar la información crítica y cerrar el sistema de forma ordenada. Los SAI ofrecen, además de protección frente a cortes de corriente, protección frente a cambios bruscos de voltaje, rayos, sobrecargas y cortocircuitos. En áreas con suministro eléctrico inestable, un SAI ahorrará muchas horas de trabajo perdido por culpa de apagones inesperados. Los hay por precios muy asequibles.

- Si a pesar de todo no puedes permitirte un SAI, debes considerar otras estrategias. Al fin y al cabo, no hay que olvidar que el objetivo de seguridad consiste en no perder información si se produce un corte de energía. La característica de *autorrecuperación* de la mayoría de programas puede programarse a intervalos muy cortos, por ejemplo de cinco minutos, con el fin de reducir el impacto de un apagón sobre el trabajo en curso. Disciplinarnos para grabar frecuentemente la información en aquellos programas que no lo hacen automáticamente también ayuda. Recordemos que en la gestión de la seguridad lo importante es definir el objetivo y luego implantar las medidas.

Siempre conectado

Hay personas para quienes resulta vital disponer de una conexión a Internet ininterrumpida. Así y todo, todos nos estamos volviendo cada día más dependientes de nuestra conexión a Internet. Alguno se dirá: “Esto no va conmigo, yo no soy un obseso de la Red, soy usuario ocasional, aprovecho sus ventajas, pero no vivo pensando en ello todo el día, no trabajo con ello,

no gano dinero con ello…”. ¿Estás seguro?

Todas las situaciones siguientes son casos reales: domingo por la noche, te dispones a imprimir las tarjetas de embarque para el vuelo del lunes y te encuentras con que no tienes conexión a Internet; 30 de junio, último día de pago de impuestos, por fin encuentras un rato para enviar telemáticamente la declaración de la renta y descubres que no te funciona la conexión a Internet; 23 de diciembre, estás de vacaciones en el pueblo y es el último día para sellar el paro, justo cuando tu conexión deja de funcionar. Como vemos, no hace falta ser un autónomo para depender de la conectividad.

La mejor manera de asegurar este servicio permanentemente consiste en utilizar conexiones redundantes:

- Es una buena idea contratar una segunda línea de conexión con un proveedor de servicios de Internet (PSI) diferente. Esta conexión de respaldo no tiene por qué ofrecer la misma velocidad que la principal, aunque sí debería proporcionar un ancho de banda capaz de suplir las necesidades de conectividad en caso de que la línea principal deje de funcionar. Se pagarán dos facturas al mes, pero se obtiene a cambio la paz de espíritu que proporciona el saber que siempre se dispondrá de conectividad.
- Otra posibilidad más versátil consiste en disponer de una línea móvil 3G que puede sacarnos del apuro en caso de emergencia. Además, puede utilizarse cuando se está fuera de casa. Por supuesto, la movilidad tiene un precio elevado.
- Si te llevas bien con tus vecinos, siempre que utilicéis proveedores diversos podéis acordar de antemano un plan de emergencia por si alguno se queda sin conexión. Para salir del apuro, podéis compartir la Wi-Fi hasta que se solucione el problema. Haberlo hablado previamente agilizará las negociaciones si se produce el

desastre.

- Infórmate de si hay algún cibercafé, locutorio con Internet o Work Center junto a tu vivienda, de los precios que cobran, de si puedes conectarte con Wi-Fi con tu portátil, etc. Saberlo por adelantado te ayudará el día que puedas necesitarlo.

Si valoras estar siempre conectado, ten preparado un plan B.

Prevención de riesgos físicos

Santa Pola, Alicante, agosto de 1998. El ordenador está ubicado en el garaje. Dentro hace más de 40 grados. Súbitamente, la tarjeta controladora de disco hace ¡pof! La pobre no ha podido resistir más el calor. Sin ordenador para el resto de las vacaciones.

Tampoco hay que olvidar los riesgos físicos como calor o humedad excesivos, inundaciones, lluvias, incendios, robos, etc.

- Mantén los equipos informáticos (ordenadores, *routers,* impresoras, discos multimedia, etc.) en un lugar fresco y seco, con aire acondicionado en verano.
- Asegúrate de despejar las ranuras de ventilación de los equipos y limpia el polvo de vez en cuando.
- Busca la mejor colocación de los equipos sobre los muebles: nunca en bordes de mesas y estanterías, siempre lo más protegidos posible frente a golpes y movimientos bruscos.
- Organiza los cables en mazos y mantenlos fuera de zonas de paso para evitar roturas por caída (y accidentes familiares).
- Ubica los equipos lejos de zonas húmedas, como cocinas y baños, y a salvo de productos nocivos, como aceites, ensaladas, refrescos, café o potentes limpiadores.

- Los incendios representan una de las amenazas más serias y peligrosas. No deja de sorprender que sean muy pocos los hogares españoles que tengan un extintor, ni siquiera en la cocina. Se trata de un grave riesgo de seguridad. Adquiere un extintor de tipo ABC, capaz de extinguir fuegos de clase A (combustibles sólidos), de clase B (combustibles líquidos) y de clase C (eléctricos). Además de los extintores, puede evaluarse la conveniencia de instalar un sistema manual o automatizado de extinción de incendios. Utilizar discos duros extraíbles facilita salvar los datos en caso de incendio: se extrae el disco con toda rapidez y se abandona al fuego el resto del equipo.
- Habla con tu aseguradora para negociar condiciones para la inclusión de tus equipos informáticos en un seguro multirriesgo para el hogar, con el fin de protegerlos tanto frente a desastres domésticos como frente a un robo.

Protección de la privacidad y del anonimato

Las películas de ciencia-ficción suelen ofrecer visiones distópicas del futuro. Una de las peculiaridades que más me llamó la atención en *Minority Report* fue el seguimiento que se hacía de los ciudadanos identificándolos gracias a los ojos. Si bien no hemos llegado a esos extremos en el mundo físico, Internet pone al alcance de empresas y gobiernos las herramientas orwellianas para conseguirlo. La intimidad en Internet no existe. Pero podemos usar herramientas para atenuar nuestro desvalimiento.

Cifrado de archivos

Cuando uno viaja y se aloja en hoteles, con frecuencia se encuentra una caja fuerte en el armario, en la cual depositar los efectos personales de mayor valor. Una vez dentro de nuestra habitación, cualquiera podría llevarse

nuestro pasaporte o dinero en efectivo si se dejaran en la mesilla. La caja fuerte con su combinación ofrece una barrera extra de protección.

Del mismo modo, los archivos en nuestro disco duro son fácilmente legibles para cualquiera con acceso a los mismos: un *ciberatacante,* un ladrón que haya hurtado nuestro portátil o un compañero de piso. La manera como podemos, por así decir, guardar nuestros archivos en una caja fuerte es gracias a la criptografía.

La criptografía, definida por el diccionario de la Real Academia Española como el "arte de escribir con clave secreta o de un modo enigmático", nos proporciona técnicas de cifrado de datos que transforman un texto en claro en un texto ininteligible para quien carezca de la clave de cifrado. Si la técnica empleada es robusta, una vez cifrado el archivo será imposible obtener la información original a no ser que se posea la clave. La criptografía no impide que alguien obtenga los archivos; lo que impide es que puedan leerlos si los obtienen y no conocen la clave.

Nuevamente, los sistemas operativos más utilizados en el hogar ofrecen herramientas de cifrado de los archivos del disco duro: EFS para el sistema de archivos y BitLocker para el disco duro en Windows, FileVault en Mac y diversas utilidades para Ubuntu. Puedes consultar la ayuda de tu sistema operativo para aprender su funcionamiento.

Existen además programas gratuitos creados por terceros con características diferentes a las de las herramientas proporcionadas por el sistema operativo, los cuales pueden ser interesantes para usuarios más avanzados. Uno de los más populares, disponible para las tres plataformas (Windows, Mac y Linux), es TrueCrypt.

En definitiva, si deseas proteger tus archivos de ojos indiscretos dentro y fuera del hogar, cífralos.

¿Sabías que cuando borras un archivo, en realidad no lo borras? Incluso aunque lo elimines de la Papelera de reciclaje, sigue en el disco duro por un tiempo indeterminado: días, semanas o años. En realidad, cuando borras un archivo éste no se destruye, sino que solamente desaparece la referencia a la ubicación del archivo en el disco, no sus datos. Con herramientas especializadas podría recuperarse la información de archivos borrados en el pasado cuyo espacio aún no haya sido sobrescrito.
Existen programas para Windows que permiten borrar la información del disco sin posibilidad de ser recuperada. Si quieres borrar a conciencia los archivos comprometidos, usa utilidades como Eraser. Los usuarios de Mac cuentan con la opción “Vaciar la papelera de forma segura” del Finder y los usuarios de Linux, con el comando “Shred”.

Anonimato en Internet

Cuando utilizas tu navegador para explorar la Red, y por ende cualquier programa que utilice servicios de Internet, revelas inevitablemente tu dirección IP. Una persona firmemente determinada, y con los recursos adecuados, puede llegar hasta tu identidad real simplemente a partir de ese dato, ya que queda registrado de manera rutinaria en todos los sitios web que visitas.

Si deseas navegar o utilizar cualquier servicio de Internet sin que el servidor al que te conectas llegue a conocer tu verdadera dirección IP, puedes conseguirlo mediante el uso de un servicio de navegación anónima o *anonimizador*. Los anonimizadores actúan como intermediarios entre tu navegador y los sitios web visitados.

El funcionamiento es muy sencillo. Te conectas con tu navegador al anonimizador, cuya interfaz es muy similar a la de los buscadores, introduces el URL de la página que deseas cargar anónimamente y ordenas al anonimizador que se adentre en la Red en busca de la página en lugar de hacerlo desde tu propio navegador. Cuando el anonimizador la haya recuperado, te la presentará en tu navegador como si nada especial hubiera sucedido. Si posteriormente a lo largo de tu sesión de navegación vas siguiendo enlaces de una página a otra, todas las nuevas páginas visitadas se

presentarán asimismo a través del anonimizador.

La mayoría de servicios de anonimato ofrecen dos versiones: una gratuita, de características básicas, y otra de pago, de superiores prestaciones. Algunos de los más populares son The Cloak, Guardster, @anonymouse o Megaproxy.

Una nota final de cautela: téngase en cuenta que el anonimizador ve y registra la totalidad de las sesiones de navegación realizadas a través de él. Por esta razón, nunca se deberían utilizar estos servicios para comprar por Internet y/o conectarse a sitios que requieran autenticación de usuario/contraseña.

Por otro lado, nuestra navegación va dejando un rastro de información sobre los sitios que hemos visitado, los archivos que hemos descargado e incluso lo que hemos escrito en formularios, todo ello en forma de historial, cookies, caché, sesiones, contraseñas, etc. Consulta la ayuda de tu navegador para aprender a borrar todos esos rastros después de cada sesión de navegación o cada cierto tiempo. También existen herramientas gratuitas de terceros, como IE Privacy Keeper, especializadas en borrar todo rastro del uso de Internet y del ordenador.

Control de acceso a equipos y archivos

Todos los sistemas operativos modernos proporcionan herramientas para controlar quién tiene acceso a qué. Debemos sacarles el máximo partido para aumentar la seguridad de nuestra información frente a incidentes debidos a causas externas o internas.

1. Crea una cuenta para cada usuario del equipo. No conviene que todos los miembros de la familia utilicen el mismo usuario, sino que cada uno posea el suyo con su propio perfil. Incluso si eres el único usuario del equipo, crea dos cuentas: una de administrador y

otra para ti.

2. Protege cada cuenta por una contraseña. Cuanto más larga y compleja sea ésta, mejor. Si en tu contexto existe la posibilidad de que alguien intente acceder a tu cuenta probando distintas contraseñas, utiliza las directivas de seguridad de contraseñas del sistema operativo para protegerte frente a estos ataques. Busca en la ayuda cómo hacerlo.
3. Asigna privilegios de administrador a una sola cuenta de usuario. Ésta debería utilizarse raramente: para instalar *software* o para realizar tareas administrativas para las que se exigen privilegios de administrador. Nunca utilices esta cuenta para realizar actividades cotidianas como navegar, leer el correo o *chatear*.
4. Aprende a utilizar los permisos de carpetas y archivos para restringir el acceso a los mismos. Una forma de mejorar la seguridad consiste en que cada usuario sólo pueda acceder a sus propios archivos, salvo el administrador, que podrá acceder a los de todos. Los permisos típicos incluyen leer, escribir y borrar. Algunos permisos dependerán del tipo de archivo, como el de ejecutar. Esta medida limita drásticamente el daño que puede hacerse desde la cuenta de un usuario, ya sea porque éste lo intente deliberadamente, ya sea porque haya sido comprometida por un *ciberatacante* o por *malware*. Eso sí, no olvides que estos permisos pueden saltarse apagando y reiniciando el ordenador desde la unidad de DVD con discos de recuperación o con otros sistemas operativos, como por ejemplo con los famosos Live DVD de Linux. Si de verdad quieres proteger la información frente a ojos indiscretos, cífrala.
5. Controla la ejecución de *software* en tus equipos, tanto para

protegerte frente a *malware* como para limitar lo que otros usuarios pueden ejecutar. Windows XP y Vista incorporan las directivas de restricción de *software,* reemplazadas en Windows 7 por AppLocker. Aprende a usarlas.

Resumen

Los cortafuegos, los antivirus y las actualizaciones son como el ABC de la seguridad, las medidas básicas que no pueden faltar. Pero nos acechan otras muchas amenazas y molestias, y para cada una de ellas existe una cura. En este capítulo se ha dado un breve repaso a qué es el *spam,* el *spyware* y cómo protegerse frente a ellos y los contenidos inadecuados; cómo estar preparado ante los fallos informáticos, de alimentación eléctrica, de conexión a Internet y otros pequeños desastres domésticos; cómo proteger la privacidad y el anonimato gracias a la navegación anónima, el cifrado de la información y el control de acceso a equipos y archivos. Sigue las recomendaciones que mejor se ajusten a tus necesidades y tu seguridad aumentará a niveles que nunca hubieras imaginado.

CAPÍTULO 5

Seguridad en redes inalámbricas Wi-Fi

Recuerdo con nostalgia el primer teléfono con el que jugué de niño, construido con dos botes de yogurt unidos por un hilo. Años después me regalaron unos *walkie talkies* de juguete para hacer de agente secreto, gracias a los cuales podíamos comunicarnos sin hilos. ¡Qué maravilla! ¡Qué libertad!

Las primeras redes de ordenadores usaron el cable para conectar unos equipos con otros. Su mayor inconveniente radica en la necesidad de extender el cable a través de habitaciones, haciendo agujeros y rozas o grapándolo a lo largo de marcos y rodapiés. Sin embargo, desde la aparición de las redes inalámbricas Wi-Fi, ¡se acabó la tiranía del cable! Proporcionan en cualquier lugar de la casa conexión a Internet y entre sí a los dispositivos más variados: ordenadores de sobremesa, portátiles, PDA, Wii, videoconsolas, discos multimedia, etc.

Por desgracia no todo son ventajas. La velocidad de transmisión de datos es mucho más lenta que con cable y, más importante, mal configuradas presentan importantes problemas de seguridad. Este último aspecto constituye el objeto de este capítulo.

Riesgos de las redes Wi-Fi

¿Dónde reside el peligro de una red Wi-Fi? ¿Por qué deberíamos preocuparnos? Cuando los equipos y el *router* de conexión a Internet utilizan todos cable, los *ciberatacantes* sólo disponen de un punto de

entrada: a través del *router*. Sin embargo, una red inalámbrica configurada incorrectamente plantea nuevos problemas de seguridad añadidos:

- Pérdida de rendimiento: un vecino gorrón podría utilizar nuestra red inalámbrica para conectarse a Internet sin pagar. Si además utiliza aplicaciones que consumen gran ancho de banda, como las descargas de archivos tipo eMule, podríamos ver peligrar nuestra propia conexión a Internet.
- Pérdida de confidencialidad: cualquier vecino o persona que pase cerca de nuestra casa podría espiar todo el tráfico que circule por nuestra red. Después de todo, Wi-Fi funciona en esencia como una estación de radio, transmitiendo la información a través de las ondas, las cuales puede captar cualquiera con una antena dentro del rango de alcance. En tal caso, el atacante podría ver todas las páginas web que visitamos y lo que escribimos en los formularios; podría leer todos los correos electrónicos que enviamos o recibimos; podría escuchar nuestras conversaciones telefónicas a través de programas como Skype; perderíamos, en definitiva, toda nuestra intimidad en el uso de Internet. Todo lo que no viaje cifrado puede ser interceptado.
- Facilidad de ataque: un *ciberatacante* podría hacer un barrido para intentar detectar los equipos de nuestra red con el fin de penetrar en ellos explotando posibles vulnerabilidades. Podría acceder a archivos en carpetas compartidas. Es como si le dejáramos la puerta abierta invitándole a colarse dentro.
- Comisión de fraudes: un *ciberdelincuente* sentado en un banco delante de nuestra casa podría utilizar nuestra red desprotegida para perpetrar desde ella acciones delictivas sin dejar huellas incriminatorias. Como resultado, en el caso de una investigación

policial, todo el rastro conduciría hasta nosotros.

Nociones básicas sobre redes Wi-Fi

Las redes inalámbricas pueden trabajar en dos modos de funcionamiento distintos: infraestructura y *ad hoc*.

Redes en modo infraestructura

En una red inalámbrica doméstica típica el *router* de conexión a Internet funciona asimismo como punto de acceso inalámbrico (WAP o simplemente AP) para todos los equipos de la casa. Esta configuración se denomina *red en modo infraestructura*. El punto de acceso actúa de puente entre ambas redes, Internet y la red inalámbrica doméstica, coordinando la transmisión y recepción de los diferentes dispositivos inalámbricos. Dependiendo del número de dispositivos que pueda servir un solo punto de acceso, se podrán ir añadiendo más a medida que sean necesarios. Teniendo en cuenta que pueden cubrir un rango de entre 25 y 100 metros, un solo punto de acceso suele bastar para el hogar.

En la jerga Wi-Fi, los dispositivos inalámbricos, ya sean ordenadores de sobremesa, portátiles o de mano, se denominan *estaciones*. Cuando se enciende una estación, lo primero que debe hacer es identificar los puntos de acceso y redes disponibles a su alcance. Los puntos de acceso emiten tramas faro para anunciar su presencia, indicando su nombre o SSID *(Service Set Identifier)*. Todos hemos visto en un ordenador el listado de redes dentro de alcance que aparece en la ventana de conexión, como en la figura 4. Cuando la estación detecta uno, se procede a la fase de autenticación, en la cual se verifica la identidad mutua. Durante esta fase se nos pedirá una contraseña si la red está protegida. A continuación se produce la asociación, que permite que el punto de acceso y la estación se intercambien información. Una vez completada la asociación, la estación ya

puede enviar y recibir paquetes. Todo el tráfico de red de las estaciones pasa a través del AP, tanto si va dirigido a Internet como a otras estaciones de la misma red. De esta forma se consigue que dos estaciones que no están al alcance una de otra, pero sí cada una dentro del radio del AP, puedan comunicarse entre sí.

FIGURA 4
Listado de redes inalámbricas dentro de alcance.

Redes en modo 'ad hoc'

Las redes *ad hoc* o de equipo a equipo están creadas exclusivamente por los propios dispositivos inalámbricos, sin ningún punto de acceso ni controlador central. Cada dispositivo se conecta directamente con otros dispositivos en la red sin pasar por un punto central. Esta topología resulta especialmente útil cuando se necesita que un pequeño grupo de ordenadores se conecten entre sí, pero sin necesidad de acceso a otra red ni de salida a Internet.

El funcionamiento de una red *ad hoc* es muy similar al descrito anteriormente para las redes en modo infraestructura. En este caso, una de las estaciones debe asumir el papel de AP, emitiendo tramas faro que permitan que otras estaciones se enganchen a la red. Algunas mejoras proporcionadas por el AP ya no están presentes, como la posibilidad de comunicar dos estaciones fuera de alcance. Si las estaciones desean acceder

a Internet, una de ellas deberá tener una segunda tarjeta de red y actuar como pasarela de acceso a Internet *(proxy)*.

Cómo proteger nuestra red Wi-Fi

Afortunadamente para el usuario doméstico, configurar una red inalámbrica de manera segura es muy sencillo. Se deben seguir los siguientes procedimientos:

Eliminar todos los valores predeterminados de la red.

Activar el cifrado de datos con un protocolo seguro.

Cerrar la red a dispositivos ajenos.

No más valores predeterminados

Si uno saca el *router* inalámbrico de la caja, lo enciende y empieza a trabajar, es verdad que las cosas funcionan sin necesidad de hacer mucho más, pero todos los valores utilizados, como por ejemplo el identificador de servicio o SSID y la contraseña de administrador, serán los predeterminados de fábrica, conocidos por todo el mundo.

Por lo tanto, el primer paso tras la configuración del punto de acceso consiste en cambiar su SSID predeterminado por uno de nuestra elección, que además no revele excesiva información. No conviene utilizar nombres propios de personas, ni de la marca del producto, ni nombres similares que anuncien a un intruso la naturaleza del blanco. Cuanto más complejo y raro sea el SSID, mejor.

Otro valor predeterminado problemático es el de la contraseña de la aplicación de administración del *router* inalámbrico. Si bien algunos proveedores de acceso a Internet no utilizan la misma contraseña para todos los *routers,* el algoritmo de generación de contraseñas suele ser conocido y reproducible con facilidad por cualquier atacante. Cualquier equipo conectado al *router* que conozca el valor de la contraseña podrá iniciar una

sesión como el administrador, con el consiguiente riesgo para la red. En cuanto hayamos configurado el *router,* debemos cambiar dicha contraseña por una robusta: más de doce caracteres con mezcla de mayúsculas, minúsculas, números y algún carácter no alfanumérico. Eso sí, es muy importante no olvidarla.

Algunos *routers* inalámbricos permiten por defecto su configuración desde Internet, no sólo desde otros equipos de la red local. Conviene desactivar esta característica, ya que expone nuestro *router* a ataques de fuerza bruta para obtener la contraseña de administrador.

Blindaje de las comunicaciones mediantcriptografía robusta

En cierto modo, cuando los equipos se conectan con el punto de acceso inalámbrico es como si estuvieran todos en un bar hablando a gritos con el camarero: éste se entiende con todos, pero también el resto de parroquianos escuchan la conversación. En otras palabras, no existe ninguna privacidad. La única forma de alcanzar con una red inalámbrica la seguridad que proporciona una red de cable es recurriendo al cifrado de las comunicaciones. Existen varios procedimientos de cifrado incorporados en prácticamente todos los equipos inalámbricos hoy en día, pero no todos son igual de seguros.

El primero fue WEP *(Wired Equivalent Privacy)*, diseñado con tantas prisas que salió al mercado infestado de agujeros de seguridad. Existen en Internet numerosas herramientas y manuales sobre cómo romper este protocolo en cuestión de minutos, por lo que ya no resulta seguro en absoluto. Mejor WEP que no usar nada, eso es verdad, pero, total, por el mismo precio conviene configurar un protocolo seguro.

En un afán por corregir las desastrosas vulnerabilidades de WEP, se crearon nuevos procedimientos de cifrado, como WPA *(Wi-Fi Protected Access)* y WPA2, este último más seguro que su predecesor. Ambos

permiten configurarse en una red doméstica utilizando la característica de compartir las claves de cifrado entre el AP y las distintas estaciones, lo que se conoce como PSK *(Pre-Shared Ke*y*)*. Aunque el estándar WPA2 se ratificó en el 2004, todavía es posible encontrar dispositivos inalámbricos, puntos de acceso y tarjetas de red que, por el motivo que sea, antigüedad o economía, no lo soportan. Ni que decir tiene que si nuestro punto de acceso y estaciones soportan WPA2 es la opción de cifrado que debemos configurar. Hoy por hoy no hay forma de romper un cifrado WPA2 en un tiempo razonable, siempre y cuando se utilicen claves muy, muy robustas.

Resumiendo: usa cifrado. Si está soportado en todos los dispositivos, que sea WPA2; en caso contrario, WPA; y si tampoco es posible, entonces WEP. Pero nunca, nunca dejes tu red inalámbrica desprotegida. De todas las recomendaciones de seguridad, ésta es la más importante. La única medida de seguridad verdadera que puedes adoptar con una red Wi-Fi consiste en cifrar las comunicaciones.

Cerrando la red a los intrusos

Dado que en cierto sentido el SSID puede considerarse como una clave secreta que identifica a la red, no conviene que sea radiada a los cuatro vientos. Conviene que el punto de acceso no se anuncie identificándose por su SSID. Aunque la ocultación del SSID no sea en buena ley una medida de seguridad fiable, si tu punto de acceso lo permite, conviene que prohíbas su multidifusión *(broadcasting)*. A pesar de todo, ocultar el SSID no es una verdadera medida de seguridad: un atacante habilidoso podrá descubrir el SSID de una red, pero mejor si ésta no lo difunde. Así elevas el listón de seguridad requerido para atacarte.

Direcciones MAC

Los adaptadores de red o tarjetas de red, inalámbricas o no, poseen una dirección física única conocida como dirección MAC (Media Access Control). Cuando dos

dispositivos de la misma red se comunican, utilizan la dirección MAC para enviarse tramas de bits de uno a otro. La dirección MAC de una tarjeta funciona en cierto sentido como el número de bastidor de un vehículo, identificándola unívocamente, con la importante diferencia de que es muy sencilla de modificar por un atacante habilidoso.

Otra medida de seguridad que puedes implantar siempre que venga soportada por tu AP consiste en filtrar los clientes que pueden conectarse a tu red en función de su dirección MAC. La mayoría de los AP permite especificar una lista de direcciones MAC permitidas. Aunque tampoco se trata de una verdadera medida de seguridad, pues la citada lista podría obtenerse con el tiempo con herramientas de *hacking* de libre distribución y luego puede ser utilizada para configurar la dirección MAC de una estación ajena, se trata de otra barrera adicional que se lo pondrá más difícil al intruso casual sin conocimientos de *hacking*. Algunos *routers* modernos utilizan este tipo de filtrado MAC bajo el espectacular nombre de *easypairing* (fácil emparejamiento). Recuerda que aunque pone las cosas más difíciles, no añade verdadera seguridad a tu red.

Otra recomendación básica es apagar el *router* inalámbrico mientras no se use. Sin duda, el remedio más eficaz para dejar fuera a los atacantes, además de ahorrar energía.

Finalmente, consulta en tu manual cómo configurar la red inalámbrica para que sólo pueda funcionar en modo infraestructura y no en modo *ad hoc*.

Resumen

Las redes inalámbricas gozan de gran popularidad en entornos domésticos gracias a la gran facilidad de instalación y comodidad de uso. Permiten conectar numerosos dispositivos a Internet y entre sí sin necesidad de tirar ni un solo cable. Pero sus ventajas palidecen al lado de sus problemas de seguridad, siempre y cuando no se implanten las contramedidas descritas.

La única protección verdadera consiste en cifrar todo el tráfico mediante WPA2. Si WPA2 no estuviera disponible en todos los dispositivos, entonces utiliza WPA. Pero nunca dejes tu red inalámbrica sin protección.

CAPÍTULO 6

Uso responsable de Internet

En Internet podemos hacer lo mismo que en el mundo real: buscar información, charlar con otra gente, enviar y recibir mensajes, obtener música, películas y libros, comprar y vender, expresar nuestras ideas y dar rienda suelta a nuestros talentos, ligar, jugar, participar en foros y comunidades, hablar por teléfono, etc. Internet funciona como un confortable universo paralelo: podemos adentrarnos en él y adoptar una personalidad virtual desde la intimidad del hogar. Precisamente esta falsa sensación de seguridad nos vuelve incautos y confiados en exceso. Este capítulo repasa un conjunto de medidas de seguridad para usar Internet con responsabilidad.

Según los estudios publicados por INTECO, los tres usos principales a los que tanto padres como hijos destinan el ordenador y la conexión a Internet en el hogar son:

- Navegación por Internet, ya sea para buscar información, conectarse al banco, realizar compras de artículos y reservas de viajes y espectáculos, o por puro ocio: ver películas y series, escuchar música, jugar, ligar, etc.
- Mensajería electrónica, tanto mensajes de correo como mensajes instantáneos.
- Descarga de archivos: los programas de intercambio de archivos

entre iguales (*Peer-To-Peer* o P2P) permiten compartir archivos entre distintos equipos conectados a Internet, de manera que unos usuarios pueden descargar los archivos del tipo que sea compartidos por otros usuarios de la red. BitTorrent y eMule se erigen como los dos buques insignia en lo que a redes P2P se refiere.

Navegación por Internet

La navegación por Internet es sin duda el servicio estrella. Tanto es así que muchos usuarios confunden Internet con navegar. Aclaremos esta confusión: Internet es una red de redes sobre la que se prestan innumerables servicios: navegación por páginas web, correo electrónico, *chat,* descarga de archivos, juegos en red, telefonía, etc. La navegación es uno más de los múltiples servicios ofertados en Internet. Si bien las posibilidades de la navegación son infinitas, los usos más frecuentes a que se destina el navegador son:

- Compras por Internet.
- Redes sociales.
- Banca electrónica.
- Búsqueda de información, para ocio o trabajo.

Compras por Internet

No debemos tener miedo a comprar por Internet en comercios de reconocido prestigio. Sin ir más lejos, yo continuamente compro libros, cómics, discos, películas, entradas de cine y espectáculos, artículos de electrónica, billetes de avión y tren, y jamás he tenido ningún problema de ningún tipo. En alguna ocasión el género llegó defectuoso o equivocado, siendo cambiado por otro inmediatamente tras mi reclamación.

Cuando vayas a comprar en Internet sigue estos consejos de sentido común:

- Debes comportarte en Internet como en el mundo físico. Si compras un DVD a un mantero o un reloj a un vendedor ambulante no puedes esperar ninguna garantía, ni que vayas a encontrarlos al día siguiente para reclamarles en caso de problemas. Del mismo modo, en Internet debes desconfiar de comercios de dudosa reputación o que no incluyen más información de contacto que una dirección de correo electrónico. En cambio, gozarás de grandes garantías si compras en comercios de reputación asentada, aunque no posean sucursales físicas.
- Desconfía de los chollos, de las superofertas y de los sitios sospechosos. Si parece demasiado bueno para ser verdad, entonces no es verdad. Si el sitio no te inspira confianza, no compres en él. Busca en foros, infórmate antes, especialmente si vas a desembolsar mucho dinero. Reflexiona. Compara precios y comercios. Recapacita antes de comprar. No seas impulsivo.
- Sufrimos un miedo irracional a usar nuestra tarjeta de crédito en Internet pero, paradójicamente, la entregamos alegremente en el restaurante o en el peaje, e incluso la revelamos por teléfono para reservar entradas u hoteles. Esta conducta no tiene ningún sentido. Siempre y cuando vigilemos con frecuencia los movimientos de nuestra tarjeta en busca de cargos indebidos, no correremos ningún peligro usándola en Internet. En caso de uso indebido, no tenemos más que anular el cargo y será el comercio el que cargue con el fraude, nunca el usuario. Si te preocupa especialmente que *ciberdelincuentes* puedan robarte su número, prueba a utilizar *tarjetas virtuales.* Todos los bancos las ofrecen, infórmate en el

tuyo. Se trata de números de tarjeta de crédito válidos asociados a tu tarjeta real, con una fecha de caducidad de un mes y con un importe máximo preasignado. Su única limitación reside en la imposibilidad de adquirir bienes que para poder retirarlos haya que presentar la tarjeta de crédito utilizada en la compra, como por ejemplo, las entradas de cine.

- En la medida de lo posible, haz la compra en sitios (mal llamados) seguros, es decir, aquellos que utilizan SSL para transmitir la información sensible. SSL constituye un requisito imprescindible a exigir en toda transacción a través de Internet que involucre el envío de información sensible, como contraseñas o números de tarjeta de crédito. Acuérdate de verificar siempre la información del certificado digital.
- No reveles excesiva información personal. Nunca des más datos de los estrictamente necesarios para pagar la compra y que ésta llegue a tu casa.
- Nunca reveles contraseñas. Nadie te pedirá jamás legítimamente ni por correo ni por teléfono las contraseñas de acceso a comercios electrónicos ni de tu banco ni de ningún otro sitio.
- Infórmate sobre los procedimientos de reembolso, cancelación y quejas. Si no aparece información sobre estos asuntos, solicítala al comercio. La manera en que informen sobre el particular ya te dará una indicación de su seriedad.
- Guarda copia de todos los correos, justificantes, albaranes y recibos que se generen durante la transacción. Constituirán tu prueba en caso de reclama- ciones.

SITIOS SEGUROS

¿Qué significa eso de sitio seguro? Simplemente, que usa un canal protegido mediante SSL para cifrar todo el tráfico entre tu ordenador y el servidor web. SSL (Secure Sockets

Layer) es un protocolo de propósito general para establecer comunicaciones seguras, propuesto en 1994 por Netscape Communications Corporation junto con su primera versión del Navigator.

El funcionamiento de SSL puede compararse con el de un furgón blindado utilizado para enviar unos documentos por ejemplo desde tu casa al banco, de manera que durante el trayecto resulte imposible hacerse con esos datos. Sin embargo, este enfoque, aunque práctico y fácil de implantar, no ofrece una solución comercialmente integrada ni totalmente segura. SSL deja de lado demasiados aspectos para que pueda ser considerado la solución definitiva:

• Sólo protege transacciones entre dos puntos: el servidor web y el navegador del comprador. No obstante, una operación de pago con tarjeta de crédito involucra como mínimo tres partes: el consumidor, el comerciante y el emisor de tarjetas. SSL carece de capacidad para completar el proceso comercial: verificar la validez del número de tarjeta recibido, autorizar la transacción con el banco del cliente y procesar el resto de la operación con el banco adquirente y emisor. Para todas estas operaciones suelen utilizarse en España los TPV (Terminal de Punto de Venta) virtuales.

• No protege al comprador del riesgo de que un comerciante deshonesto utilice ilícitamente su tarjeta.

• Los comerciantes corren el riesgo de que la tarjeta de un cliente sea robada o que ésta no haya sido aprobada o no tenga crédito, y normalmente se encuentran a merced de los grandes medios de pago en caso de uso ilícito de una tarjeta o ante la picaresca de algunos consumidores.

• Es importante recalcar que SSL sólo garantiza la confidencialidad e integridad de los datos privados en tránsito desde el navegador hasta el servidor, ni antes ni después. Lo que suceda con ellos en el servidor queda ya más allá de la competencia de este protocolo. Los datos podrían ser manipulados irresponsablemente por los empleados del comercio o caer en manos de un ciberdelincuente que asaltara el servidor con éxito, sucesos que se producen con alarmante frecuencia en estos días.

Resumiendo: ¿un sitio es seguro por usar SSL? ¡En absoluto! Es mezclar churras con merinas.

Redes sociales

Las redes sociales, sean éstas para el ocio o el negocio, como LinkedIn, MySpace, Facebook o Tuenti, han arrasado en los últimos años, hasta el extremo de que se llega a afirmar que si no estás en tal o cual red social, entonces no existes. Según INTECO, en España en torno al 50% de los internautas mayores de 15 años tiene su perfil en alguna red social. Al margen de las innegables ventajas que proporcionan para darse a conocer, para seguirles la pista a conocidos y amigos y para estar en contacto con personas en distintos lugares del globo, las redes sociales plantean

tremendos interrogantes de seguridad y privacidad, en especial para los más jóvenes:

- Amenazas a la intimidad y la privacidad personal y familiar: muchos usuarios exhiben impúdicamente su intimidad en las redes sociales, colgando vídeos y fotos de sí mismos que jamás enseñarían en persona. No son conscientes de su verdadero valor para terceros ni de que son vistos por millones de internautas. En los perfiles suele cargarse información de carácter personal: gustos, aficiones, ideología, religión, orientación sexual, experiencias y vivencias. Muchos de estos datos corresponden al nivel de seguridad alto según la LOPD y podrían ser utilizados por terceros de forma ilícita.
- Vulneración de la propiedad intelectual: la mayoría de los usuarios de redes sociales no lee las licencias de uso ni los términos del servicio, por lo que ignoran que ceden a la plataforma derechos plenos e ilimitados sobre las obras que cuelgan creadas por ellos mismos: fotografías, música, vídeos, etc. Estos materiales podrían ser utilizados, compartidos y difundidos a través de las redes sociales y sitios web colaborativos, con un beneficio económico para la plataforma a espaldas del usuario.
- Acceso a contenidos inapropiados: algunos usuarios de redes sociales cuelgan material que bien puede considerarse inapropiado para menores, por su contenido sexual, violento, xenófobo, vejatorio u obsceno. No todo lo que se publica en ellas está hecho para todos los ojos.
- *Ciberbullying:* según el sitio web Ciberbullying, éste "se define como acoso entre iguales en el entorno TIC, e incluye actuaciones de chantaje, vejaciones e insultos de niños a otros niños […]

Estamos ante un caso de *ciberbullying* cuando un o una menor atormenta, amenaza, hostiga, humilla o molesta a otro(a) mediante Internet, teléfonos móviles, consolas de juegos u otras tecnologías telemáticas". Por consiguiente, para hablar de *ciberbullying* deben verse implicados solamente menores, ya que si se involucran adultos pasaríamos a hablar de *ciberacoso.*

- *Grooming:* consiste, según el sitio web Pantallas Amigas, "en el conjunto de estrategias que una persona adulta desarrolla para ganarse la confianza del menor a través de Internet con el fin último de obtener concesiones de índole sexual […] Desde un acercamiento lleno de empatía y/o engaños se pasa al chantaje más cruento para obtener imágenes comprometidas del menor y, en casos extremos, pretender un encuentro en persona. El daño psicológico que sufren niños, niñas y adolescentes atrapados en estas circunstancias es enorme".
- Dificultad para darse de baja: al igual que ocurre con las compañías telefónicas, te lo ponen facilísimo para darte de alta, pero padeces un infierno para darte de baja. De hecho, el material que has colgado no se destruye al darte de baja, queda ahí, supuestamente inaccesible.

Para hacer un uso responsable de las redes sociales, se recomienda seguir los siguientes consejos:

- Nunca publiques información excesiva sobre tu vida personal y familiar. Las cosas que no comentarías en un bar o en el trabajo para que las escuchen *todos,* no las publiques en la red social, porque las leerá *todo el mundo.* Tú tienes el control sobre lo que publicas y lo que no. Ejércelo con mesura. Las empresas bucean

cada vez con mayor frecuencia en las redes sociales para obtener información sobre candidatos o empleados. No cuelgues nada de lo que puedas arrepentirte. Básicamente, la premisa que puedes seguir es: si no se lo enseñarías a tu madre, ¡no lo publiques!

- Utiliza un *nick* o pseudónimo en tu vida en Internet cuya identidad real sólo conozcan las personas más allegadas a ti. No permitas que tu identidad real pueda relacionarse con tu identidad virtual.
- Cuando cuelgues fotos, vídeos u otros materiales gráficos, respeta la privacidad de otras personas que puedan aparecer en ellos. A lo mejor a ti no te importa exhibirte borracho con los gallumbos en la cabeza, pero a otros sí. Una cosa es una noche loca y otra muy distinta que lo tenga que ver *todo* el mundo.
- Lee detalladamente las condiciones generales de uso y la política de privacidad de la red social para saber a qué atenerte: qué les autorizas a hacer con tus datos personales, qué derechos de propiedad intelectual les cedes sobre los contenidos que publicas, qué política de cancelación del contrato existe, etc.
- Configura adecuadamente el nivel de privacidad de tu perfil. Hoy en día se ha convertido en una competición el ver quién tiene más *amigos* y *seguidores* en las redes sociales. No hagas que tu perfil sea público. Ábrelo solamente a tus amigos reales de carne y hueso. Asegúrate de que no es indexado por buscadores.
- No aceptes las solicitudes de contacto que te lleguen, salvo que procedan de individuos a los que conoces previamente en persona o en Internet. Piensa que cuando agregas contactos podrán ver tu perfil, tus fotos, enviarte mensajes, y no sabes quién te está pidiendo contacto. Su objetivo puede ser inundarte con publicidad hipercontextualizada gracias a la extensa información personal de

tu perfil.

- Nunca publiques datos de contacto físicos como dirección o teléfono. Esa información sólo tiene sentido para tus amigos reales y nunca debería aparecer en tu perfil otra información de contacto que tu dirección de correo. Recuerda que debes desvincular tu vida real de tu vida virtual.
- Si utilizas herramientas de *microblogging* como Twitter, no reveles tu posición en todo momento porque podrías hacer peligrar tu integridad física. En la misma onda, cuando publiques fotos en tu vivienda o lugares donde estás localizable, no las geolocalices con coordenadas GPS. Recuerda, nadie debe poder llegar hasta tu vida real desde tu vida virtual.
- Utiliza contraseñas robustas y nunca las compartas con nadie.
- Denuncia el contenido o los usuarios que incumplan las condiciones de uso de la red social.
- Bloquea y denuncia a cualquier persona que te envíe mensajes no deseados o inapropiados.
- Las redes sociales suelen incorporar en su ayuda una sección sobre seguridad. Léela y aplica los consejos específicos para esa red social.

Banca electrónica

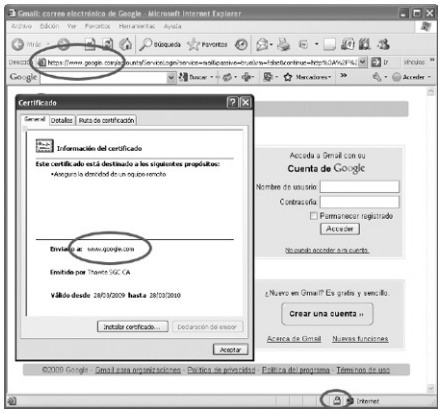
Una de las aplicaciones favoritas del navegador entre los adultos es la banca electrónica: consultar saldos, hacer transferencias, contratar productos financieros, todo ello sin moverse de casa. En los últimos años, la mayor amenaza para los usuarios de banca electrónica procede del *phishing* (véase el capítulo 2). Se ofrecen a continuación diez consejos para evitar el fraude bancario y *phishing:*

- Ignora completamente mensajes procedentes de organizaciones de las que no eres cliente.
- Aunque seas cliente, no respondas nunca a un mensaje que solicite tus credenciales o cualquier otra información personal sensible. Tu banco legítimo jamás te lo pedirá.
- Nunca acudas a un sitio web siguiendo un enlace en un mensaje. Es mejor utilizar los Favoritos o Marcadores del navegador para almacenar los sitios frecuentemente visitados.
- Observa que la dirección de la página del banco donde se te piden tus credenciales de acceso empieza por https:// y que aparece un candado cerrado en la barra de estado del navegador, indicativos de que la comunicación se está protegiendo mediante SSL. Verifica siempre los certificados digitales: comprueba que la dirección en el certificado coincide con la URL de la página en la barra de direcciones. Esta ventana se abre haciendo doble clic sobre el candadito de la barra de estado. Si aparecen mensajes de advertencia o de errores, no sigas adelante y ponte en contacto con la entidad.
- Vigila activamente los movimientos de tu tarjeta de crédito y de tus cuentas. Comunica inmediatamente a tu banco cualquier movimiento sospechoso.
- Si crees que has sucumbido víctima de un ataque de *phishing*, informa cuanto antes a tu banco.
- Mantén el equipo debidamente actualizado, con los últimos parches y actualizaciones de seguridad, tal y como se explicó en el capítulo 3.
- Instala y asegúrate de que siempre funciona actualizado un antivirus capaz de detectar, bloquear y eliminar *malware* variado:

virus, troyanos, *spyware* y demás fauna. Recuerda todo lo explicado en el capítulo 3.

- Aprende a utilizar las herramientas antifraude incorporadas en los lectores de correo y en los navegadores, capaces de detectar ataques de *phishing.*
- Utiliza un cortafuegos personal, siguiendo las instrucciones del capítulo 3.

FIGURA 5
Verifica siempre que la dirección que aparece en el URL coincide con la del certificado de seguridad.
La ventana con la información del certificado aparece haciendo doble clic sobre el candadito de la barra de estado.



Consejos generales de navegación

Además de estos usos específicos de la navegación, que plantean sus propios desafíos de seguridad, el navegador puede utilizarse con otros muchos fines, como buscar información, conectarse a *blogs,* ver vídeos, descargar *software,* etc. Al margen del uso concreto, debemos seguir los siguientes consejos al navegar:

- Mucho cuidado con las descargas de *software.* Se han dado casos de programas antivirus gratuitos que en realidad eran ¡virus!

Nunca descargues desde sitios sospechosos, sino desde los sitios oficiales. Y antes de instalar nada, ¡analízalo con un buen antivirus! En caso de duda, acude al servicio en línea de escaneo de archivos de VirusTotal.

- Al igual que con las actualizaciones del sistema operativo, mantén tu navegador siempre al día con los últimos parches de seguridad. Aprende cómo hacerlo con tu navegador concreto.
- Todos los navegadores permiten configurar opciones de seguridad. Consulta la ayuda del tuyo para aprender a configurarlo de la manera más segura posible. ¡No navegues en un cascarón lleno de agujeros!
- Configura tu navegador para bloquear las molestas ventanas emergentes *(popups)*. Si sus características no te convencen, considera instalar un programa de terceros.
- Salvo emergencias, no utilices equipos públicos para conectarte a tu banco y realizar transacciones comerciales, porque no sabes si tendrán instalado un programa *key logger,* cuya misión consiste en registrar tus pulsaciones de teclado sin que te enteres para robarte tus contraseñas. Los hay que incluso realizan capturas sucesivas de pantalla, para contrarrestar los teclados virtuales introducidos por algunos bancos.
- Nunca dejes que el navegador autocomplete las contraseñas. Busca en la configuración del mismo cómo desactivar esta característica, muy práctica, sí, pero peligrosa.
- Tampoco dejes que los sitios recuerden tus credenciales de acceso. Te habrás percatado de que la mayoría de servicios web que solicitan nombre de usuario y contraseña para iniciar sesión incluyen una casilla de verificación con un texto similar a

"Recordarme" o "No volver a pedir contraseña". Pues bien, nunca la verifiques, porque entonces cualquier persona que pudiera acceder a tu navegador podría suplantarte en ese sitio.

- Casi todas las aplicaciones web en las que es necesario identificarse para acceder al servicio (bancos, correo *web, blogs,* comercios, etc.) incluyen un botón o enlace con el nombre "Abandonar sesión", "Salir", "Terminar sesión", o sus versiones en inglés, como "Log out". Lo has visto más de una vez, ¿verdad? Pues acostúmbrate a cerrar la sesión siempre antes de cerrar el navegador. Así evitarás que alguien que utilice el mismo ordenador después de ti pueda acceder a tus datos.
- Una vez más, recuerda el consejo del capítulo 4: nunca navegues utilizando un usuario del ordenador con privilegios de administrador.
- Si te preocupa especialmente la privacidad, borra tras tus sesiones de navegación todo el rastro que hayas ido dejando: historial, *cookies,* caché, etc. Especialmente si has navegado desde un equipo de uso público. Todos los navegadores permiten hacerlo. Consulta la ayuda del tuyo para aprender cómo.

Protección de menores

Un colectivo especialmente vulnerable en Internet es el formado por los menores. Si tienes hijos, te interesará seguir las siguientes pautas para que su experiencia en Internet sea apacible y enriquecedora. Partimos de la base de que has seguido todos los consejos de seguridad mencionados en los capítulos 3, 4 y 5 para proteger el equipo desde el cual se conectarán a Internet.

- Instala el ordenador en una sala común donde puedas ver qué

hacen tus hijos con él. Si no puedes estar presente mientras navegan, considera seriamente instalar algún programa de vigilancia para saber lo que han hecho con el ordenador, como Windows Protección Infantil o el control parental de Mac OS X. Los informes de actividad detallados de tus hijos te muestran todos los sitios web que visitan (o intentan visitar) y si un sitio se ha permitido o bloqueado.

- No permitas que tus hijos utilicen cámara web *(web-cam)* si no estás delante. Enséñales a hacer un uso responsable de la misma.
- Establece unas reglas consensuadas claras y razonables sobre qué usos del ordenador y de Internet son aceptables y cuáles no, por qué sitios se puede navegar y cuáles están prohibidos, etc.
- Aprende sobre informática y seguridad más que ellos. Mantente siempre un paso por delante, para que puedas asesorarles, protegerles y… ¡que no te la jueguen!
- Familiarízate con las aplicaciones y mundos virtuales que visitan tus hijos, para advertirles de posibles riesgos, como en el caso de las redes sociales o de la mensajería instantánea.
- Cuando se solicite una dirección de contacto en las aplicaciones en las que se registra tu hijo, establece tu correo electrónico como dirección secundaria de contacto para estar informado de los mensajes que le llegan.
- Instala *software* de control de contenidos, como el descrito en el capítulo 4, o configura el del sistema operativo, si éste lo incorpora, como en el caso de Windows Vista, Windows 7 o Mac OS X Leopard.
- Internet es muy beneficioso para el desarrollo intelectual y social del niño, pero como con cualquier otra actividad (televisión,

videojuegos, lectura, etc.) debes limitar el tiempo de conexión. Es muy recomendable prefijar un horario para el uso del ordenador y de Internet.

- Habla con ellos sobre lo que hacen en Internet, qué les gusta más, comenta sus experiencias, anímales a que te consulten con sus problemas o dudas. Hazles comprender que tú eres la persona a quien acudir en caso de que ocurra un incidente, para lo cual, obviamente, deberás ganarte su confianza.
- Conciénciales mínimamente en seguridad. Explícales que nunca deben revelar información personal: ni física, como su domicilio o teléfono, ni virtual, como contraseñas o nombres de usuario. Revisa periódicamente sus perfiles para asegurarte de que no revelan información personal excesiva.
- No permitas que tus hijos descarguen nada sin tu consentimiento. Cuida especialmente la descarga e instalación de *software,* ya que podrían introducir *malware* inadvertidamente.
- Igualmente, no permitas que suban sin tu consentimiento material multimedia personal: fotos, vídeos, grabaciones en directo con la *webcam,* etc.
- Crea un usuario del sistema operativo para cada miembro de la familia y nunca jamás otorgues privilegios de administrador a tus hijos.
- Tal y como se explicó en el capítulo 3, utiliza cortafuegos, antivirus, actualizaciones y explica a tus hijos la necesidad de tales herramientas, aunque a veces resulten molestas. INTECO y Pantallas Amigas han creado SecuKid, un juego para móviles dirigido a todos los públicos, especialmente niños y adolescentes a partir de los 11 años, concebido para conocer mejor algunos

riesgos de Internet, sus efectos y cómo prevenirlos. Así aprenderán jugando.

Mensajería

El correo electrónico y el *chat* a través de programas como Messenger constituyen las aplicaciones de Internet más utilizadas después de la navegación. No hay que asustarse por que los adolescentes pasen cientos de horas "chateando". Es la nueva forma de relación social.

Correo electrónico

Muchos neófitos se han asomado al mundo de Internet a través de la ventana del correo electrónico. Quedaron deslumbrados por la mágica posibilidad de enviar un mensaje a otra persona en cualquier lugar del globo, con la seguridad de que le llegaría en segundos y a un precio casi nulo. Constituye una herramienta tan rápida, cómoda y barata que, una vez que se ha probado, ya no se puede prescindir de ella. Porque no sólo permite enviar mensajes, sino que pueden adjuntarse archivos de cualquier clase, como imágenes JPG o GIF, vídeos WMV, MPG o AVI, documentos Word, presentaciones en PowerPoint… en fin, lo que sea. No existe limitación alguna, excepto tal vez la del tamaño.

Sin embargo, con la rapidez y la conveniencia llegan también los quebraderos de cabeza. De manera misteriosa, uno no sabe muy bien por qué, pero empieza a recibir correos basura que inundan su Bandeja de entrada con publicidad vulgar, timos, *malware* y *phishing*.

Lo que comenzó siendo una sencilla herramienta para enviar texto sin más ha evolucionado hasta un nivel de complejidad que puede rebasar con facilidad a los usuarios más noveles. El uso irresponsable del correo electrónico amenaza la privacidad personal y la integridad del propio ordenador. Veamos algunos consejos para protegernos frente a estas

amenazas:

- Los ficheros adjuntos siguen constituyendo hoy en día un importante vector de infección. No abras ficheros adjuntos sospechosos que procedan de desconocidos o que no hayas solicitado. Como la mayoría de pasarelas de correo filtran el correo en busca de *malware* antes de entregárselo al usuario, con el fin de sortear esta protección muchos mensajes de correo no adjuntan un ejecutable malicioso, sino que incorporan un enlace a una página web desde la cual puedes descargarlo, burlando así las protecciones del correo. Sé consciente de esta estratagema y no descargues nada enlazado desde un correo sospechoso.
- Si el mensaje con el adjunto o el enlace al programa proviene de alguien conocido, aun así sé cauto, porque tu amigo podría estar infectado. Piensa que un virus puede autoenviarse a todos los contactos de una víctima. Acostúmbrate a analizar rutinariamente con un antivirus todo programa antes de ejecutarlo por primera vez.
- Si te sigue llegando correo basura, protégete instalando un filtro *antispam,* como se explicó en el capítulo 4.
- Los clientes de correo suelen incorporar una función conocida como Vista previa, que permite previsualizar los mensajes desde la Bandeja de entrada sin necesidad de abrirlos. Algunas muestras de *malware* se han ejecutado sin necesidad de abrir ningún archivo adjunto, ni hacer doble clic sobre nada, ni seguir enlaces. Bastaba con leer el mensaje infeccioso para quedar infectado. Si la previsualización de mensajes está activada, entonces basta con que el correo esté el primero en la Bandeja de entrada para que se ejecute automáticamente su carga maliciosa, infectando al

infortunado usuario.

- Del mismo modo, puedes ponérselo aún más difícil al *malware* si desactivas la visualización de los mensajes en HTML, donde podría ocultarse potencialmente un código malicioso.
- Sigue todas las recomendaciones que se dieron en el capítulo 4 para proteger tu dirección de correo frente a *spammers*. Cuanto mejor la protejas, menos *spam* te llegará. No se la reveles al primero que te la pida.
- Tal y como se explicó en el capítulo 4, utiliza la copia de carbón oculta cuando envíes un mensaje a múltiples destinatarios.
- Utiliza contraseñas robustas para proteger el acceso a tu cuenta de correo. Ya sabes cómo debe ser una contraseña segura: más de doce caracteres, con mezcla de mayúsculas, minúsculas, números y caracteres no alfanuméricos. Si tu servidor de correo lo permite, utiliza un canal cifrado con SSL. En el caso del correo web, asegúrate de que la página empieza por https:// y de que aparece un candadito en la barra de estado del navegador.

Mensajería instantánea

Uno de los mayores problemas del correo electrónico es que cuando se envía un mensaje no se sabe cuándo va a llegar. Lo normal es que tarde unos pocos segundos, pero aun así no se tiene certeza de cuándo lo leerá el destinatario. En estas condiciones resulta muy difícil mantener una conversación.

La mensajería instantánea (MI) se creó con el objetivo de permitir que los usuarios se comunicasen instantáneamente. Basta con saber la dirección de una persona para poder enviarle un mensaje inmediatamente. Éste se recibe al instante y se puede contestar a renglón seguido si así se desea,

permitiendo una comunicación (casi) tan fluida como la conseguida mediante el teléfono, con una o con varias personas a la vez.

"Chatear" a través de canales de charla en IRC o a través de programas como Messenger se está convirtiendo en un fenómeno social de masas, en una nueva forma de comunicación y de relación. Su facilidad de uso, la posibilidad de socializar e intercambiar archivos instantáneamente con otras personas en cualquier lugar del mundo, el no verse las caras directamente, la flexibilidad del lenguaje, las posibilidades de ligar, son sólo algunos de los factores de éxito que hacen de este servicio el más popular de la Red después del correo electrónico y de la navegación. El chat está arrasando y cada día penetra más profundamente en la neocultura internauta.

Sigue estos consejos para proteger tu privacidad cuando "chatees" usando programas de mensajería instantánea:

- Ten muy presente que el *chat* es también vehículo de timos, fraudes y *malware.* No aceptes invitaciones para visitar sitios web que te resulten sospechosos o que procedan de desconocidos.
- Todos los programas de *chat* y de mensajería instantánea incluyen alguna función para enviar archivos. Rechaza los archivos adjuntos que no hayas solicitado o que te resulten sospechosos. Si los abres, analízalos antes con un antivirus. Incluso las fotografías pueden contener código malicioso.
- Está muy bien tener muchos amigos y contactos virtuales, pero mejor si son de fiar. Sé cauto al conversar o agregar contactos desconocidos. Muchos sólo te quieren para enviarte publicidad o para robarte tu identidad.
- Los *ciberdelincuentes* utilizan multitud de canales con el fin de robar información confidencial. Está de más decir que no debes facilitar a nadie datos confidenciales (contraseñas, nombres de

usuario, datos bancarios, etc.) a través de estos canales.
- Antes o después te acosarán o molestarán a través del *chat* o del Messenger. Aprende a rechazar a los usuarios "no deseados", de los que no quieras recibir mensajes.

Descarga de archivos

Muchos usuarios españoles dieron el salto a la banda ancha precisamente para poder usar la "mula", como se conoce coloquialmente a eMule, el popular programa para compartir archivos. Se puede compartir literalmente de todo:

- Archivos de vídeo: películas de cine, documentales, series, cortos, etc.
- Archivos de música: canciones sueltas, discos, discografías completas, audiolibros, etc.
- Archivos de documento: imágenes en cualquier formato, libros electrónicos en formato PDF, cómics, documentos ofimáticos de Word, Excel, Access, etc.
- *Software:* todo tipo de programas, desde sistemas operativos a aplicaciones sencillas.
- En definitiva, cualquier archivo en formato digital.

El uso indiscriminado de programas P2P como BitTorrent o eMule plantea numerosos problemas de seguridad:

- Vulneración de la propiedad intelectual: dependiendo del tipo de contenido descargado, se pueden estar violando derechos de autor. Habrá que prestar atención a qué se descarga y comparte, por si se estuviera cometiendo alguna infracción.

- Descarga de *software* infectado: más del 50% del soft-ware disponible en redes P2P está infectado por *mal- ware,* por lo que se desaconseja completamente acudir a estas redes en busca de *software.* Es más seguro acudir a la tienda o a sitios de descarga acreditados. Por otro lado, el nombre del archivo no garantiza su contenido. Con más frecuencia de la deseada uno se encuentra con que el archivo descargado no se corresponde en absoluto con lo que se deseaba descargar.
- Filtraciones de información: estos programas funcionan compartiendo archivos en una serie de carpetas del disco duro. A menudo, por desconocimiento, los usuarios comparten todo el disco duro o una región muy grande del mismo, lo que significa que cualquier usuario de la misma red podrá descargarse cualquier archivo de su disco. Comprueba bien qué carpetas estás compartiendo, no vayas a encontrarte con sorpresas.
- Ataques de denegación de servicio (*Denial of Service*, DoS): las redes P2P se utilizan cada vez más para realizar ataques DoS, por supuesto sin el conocimiento de los usuarios.

Si utilizas la "mula" u otro programa P2P, hazlo con seguridad. No olvides poner en práctica las siguientes recomendaciones:

- Acude a la página oficial de tu programa P2P favorito para instalarlo desde ahí, no aceptes imitaciones ni te fíes de modificaciones con la promesa de descargas más rápidas.
- Analiza con un antivirus todos los archivos que te descargues con el programa P2P, tanto si son de *software* como si no. Existe *malware* que aprovecha vulnerabilidades en los programas de reproducción de música y vídeo para incluir código malicioso en

archivos multimedia aparentemente inocentes.

- No me cansaré de repetirlo: jamás utilices un usuario con permisos de administrador para ejecutar programas P2P.
- No utilices los nombres predeterminados para las carpetas donde descargar archivos, ya que buscar rutas de acceso conocidas es un recurso habitual del *malware*.
- Familiarízate con los tipos de extensión para los ficheros típicos. Una extensión de nombre de archivo es un juego de caracteres que se agrega al final de un nombre de archivo para determinar cuál es el programa que debe abrirlo. Cuando descargues, presta especial atención a la extensión de los ficheros que te bajas, ya que podrían indicar intentos de ataque: por ejemplo, un vídeo nunca tendrá extensión .EXE. Conviene que consultes la ayuda de tu sistema operativo para configurarlo de manera que nunca oculte las extensiones de los archivos.

Resumen

Navegar, enviar mensajes y descargar archivos constituyen las tres aplicaciones favoritas de los internautas españoles. El practicar estas actividades desde la intimidad del hogar nos proporciona a veces una falsa sensación de anonimato y seguridad; sin embargo, pueden representar graves riesgos para la privacidad si no se toman una serie de precauciones. Con sentido común y una profilaxis básica, podrás disfrutar al máximo de todas ellas, sin sorpresas ni disgustos. Sigue los numerosos consejos y pautas de actuación de este capítulo y tus vivencias y experiencias en Internet serán fantásticas. Internet se perfila como uno de los mayores inventos de la humanidad. ¡Disfrútalo sin temor! Y recuerda siempre que el mejor cortafuegos eres tú.

Recursos sobre seguridad en Internet

Capítulo 2

Seguridad en el hogar de Microsoft: protéjase frente al robo de identidad, *spyware* y virus: http://www.microsoft.com/spain/protect/default.mspx

Campaña contra el fraude *on line* y la seguridad en la Red: http://www.seguridadenlared.org

Alerta-Antivirus: Centro de Alerta Temprana sobre Virus y Seguridad Informática: http://alerta-antivirus.inteco.es/

OSI-Oficina de Seguridad del Internauta: http://osi.gob.es/

Capítulo 3

1. Cortafuegos personales

ZoneAlarm: http://www.zonealarm.com/security/es/zonealarm -pc-security-free-firewall.htm

COMODO Internet Security: http://personalfirewall.comodo.com/download_firewall.html

Sunbelt Personal Firewall: http://www.sunbeltsoftware.com/Home-Home-Office/Sunbelt-Personal-Firewall/

2. Antivirus

2.1. Antivirus como producto

AVG Anti-Virus Free Edition: http://free.avg.es/

BitDefender 10 Free Edition: http://www.bitdefender.es/PRODUCT-14-es--

BitDefender-Free-Edition.html

Avira AntiVir Personal Edition: http://www.free-av.com/en/products/1/avira_antivir_personal__free_antivirus.html

avast! 4 Home Edition http://www.avast.com/esp/avast_4_home.html

Malwarebytes' Anti-Malware: http://www.malwarebytes.org/mbam.php

Panda Cloud Antivirus http://www.cloudantivirus.com/default.aspx?lang=spa

2.2. Antivirus como servicio

ActiveScan 2.0 de Panda-Tu segunda opinión sobre la seguridad de tu PC: http://www.pandasecurity.com/activescan/index/

Trend Micro HouseCall-Trend Micro España: housecall.trendmicro.com/es

Software antivirus y seguridad en Internet para su equipo |McAfee: http://home.mcafee.com/Downloads/FreeScan.aspx

Norton Security Scan: http://security.symantec.com/sscv6/WelcomePage.asp

VirusTotal: http://www.virustotal.com/es/

Capítulo 4

1. Contenidos molestos o inadecuados

1.1. Lucha contra el correo basura

G-Lock SpamCombat: http://www.glocksoft.com/sc/

SPAMfighter: http://www.spamfighter.com/Lang_eS/

Spamihilator: http://www.spamihilator.com/

Mailinator: http://mailinator.com

1.2. A salvo de 'software' espía en el ordenador

Ad-Aware Free: http://www.adaware.es/fichehtml?REF=664679

Spybot S&D: http://www.safer-networking.org/es/

Windows Defender: http://www.microsoft.com/windows/products/winfamily/defender/default.mspx

1.3. Contenidos bajo control

Optenet WebFilter PC: http://www.optenet.com/es/pcwebfil ter.asp

Windows Protección Infantil: http://www.microsoft.com/latam/protect/products/family/onecarefamilysafety.mspx

2. Fallos de 'software' y 'hardware'

Copias de seguridad *on line:* http://www.banckup.net/

MAST Backup Online-Servicio de Backup & Recuperación Online: http://www.mastbackuponline.com/

3. Protección de la privacidad y del anonima

3.1. Cifrado y borrado de archivos

TrueCrypt-Free Open-Source On-The-Fly Disk Encryption Software for Windows Vista/XP, Mac OS X and Linux: http://www.truecrypt.org/

Eraser: http://eraser.heidi.ie/

3.2. Anonimato en Internet

The Cloak: http://www.the-cloak.com/

Guardster: http://www.guardster.com/@anonymouse http://anonymouse.org/

Megaproxy: https://www.megaproxy.com/freesurf/

IE Privacy Beeper: http://www.unhsolutions.net/IE-Privacy-Keeper/

Capítulo 6

INTECO-Instituto Nacional de Tecnologías de la Comunicación: http://www.inteco.es/

1. Redes sociales

LinkedIn: http://www.linkedin.com/
MySpace: http://es.myspace.com/
Facebook: http://www.facebook.es/
Tuenti: http://www.tuenti.com/
Ciberbullying. http://www.ciberbullying.net/
Pantallas Amigas. http://www.pantallasamigas.net/
Twitter: http://twitter.com/

2. Protección de menores

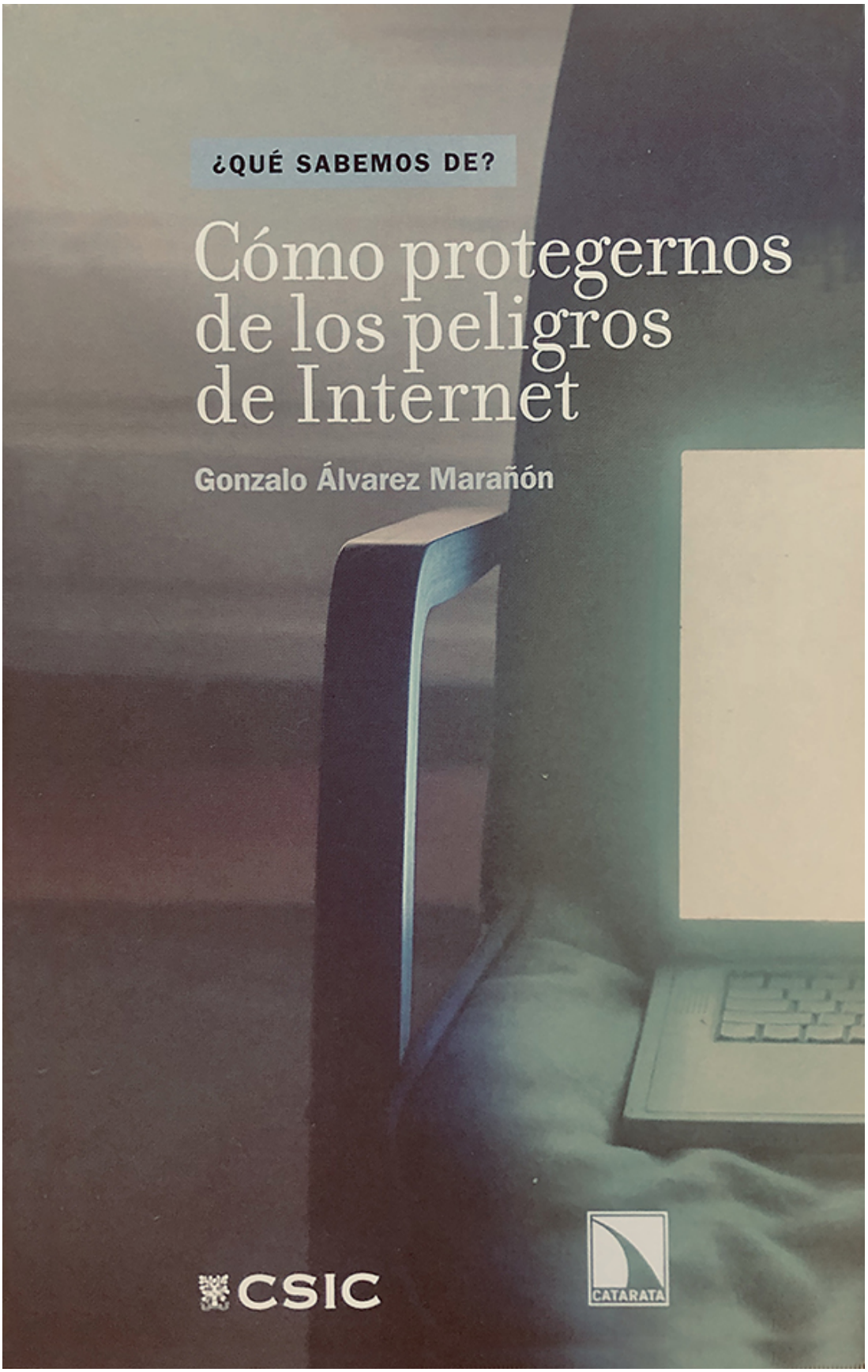
SecuKid: http://www.secukid.es/

3. Mensajería

Messenger: http://download.live.com/messenger

4. Descarga de archivos

eMule: http://www.emule-project.net/
BitTorrent: http://www.bittorrent.com/


¿QUÉ SABEMOS DE?
Cómo protegernos de los peligros de Internet
Gonzalo Álvarez Marañón
CSIC
CATARATA

Document Outline

- Cómo protegernos de los peligros de Internet
  - Créditos
  - Glosario
  - Introducción
    - Internet sí, pero con seguridad
    - Un libro para el usuario doméstico
    - Un viaje a la seguridad de la información
    - Recursos sobre seguridad en Internet
    - ¿Se te escapa algún concepto? Acude al glosario
    - Agradecimientos
  - Capítulo 1. Qué es la seguridad de la información
    - La vida es riesgo
    - Expectativas
    - Contextos
    - Contexto y expectativas en el hogar
    - Inversión en seguridad
    - No toda la información es igualmente valiosa
    - No toda la información está expuesta a los mismos peligros
    - Resumen
  - Capítulo 2. Amenazas a la información
    - ‘Ciberatacantes’
    - ‘Malware’
    - Fraudes y timos
    - Otras amenazas
    - Resumen
  - Capítulo 3. Medidas básicas de seguridad
    - Cortafuegos
    - Antivirus
    - Actualizaciones de seguridad
    - Resumen
  - Capítulo 4. Medidas avanzadas de seguridad
    - Contenidos molestos o inadecuados
    - Fallos de ‘software’ y ‘hardware’

    - Protección de la privacidad y del anonimato
    - Resumen
- Capítulo 5. Seguridad en redes inalámbricas Wi-Fi
    - Riesgos de las redes Wi-Fi
    - Nociones básicas sobre redes Wi-Fi
    - Cómo proteger nuestra red Wi-Fi
    - Resumen
- Capítulo 6. Uso responsable de Internet
    - Navegación por Internet
    - Mensajería
    - Descarga de archivos
    - Resumen
- Recursos sobre seguridad en Internet
    - Capítulo 2
    - Capítulo 3
    - Capítulo 4
    - Capítulo 6